



Protecting Texans' Identities

The Challenges of
Securing Privacy in
Transparent Government

Susan Combs
Texas Comptroller
of Public Accounts

Click.

You can't see them,
but they can see you.

Click.

They want to steal
your valuable personally
identifiable information.

Click.

They can seriously
damage your world from
a world away.

Click. Gone.

December 1, 2010

The Honorable Robert L. Duncan
State Senator, District 28
Texas Senate
1500 Broadway St., Suite 902
Lubbock, Texas 79401-3108

Dear Senator Duncan:

Texans have long cherished their right to be left alone. Few things are more precious to us than having our privacy respected and protected. In today's technological world, where data takes the form of bits and bytes, it is increasingly important that government agencies be diligent in ensuring that a citizen's personally identifiable information is not compromised.

This report examines the volume and types of personal information that Texas state government agencies collect, maintain and – in some cases – are authorized to disclose and sell.

Identity theft is a sad reality of modern life, and criminals can piece together seemingly insignificant bits of information to create a bigger picture that could place a citizen's finances, credit score or even personal safety in jeopardy.

Only two other states have a higher per capita identity theft complaint rate than Texas. Three South Texas cities – Laredo, McAllen and Brownsville – lead the nation in identity theft complaints. Of course, complaints are only filed when a citizen suspects there is a problem; many instances of identity theft may go undetected by the victims for months or years before the economic costs mount and become apparent.

In recent years, we've brought greater transparency and openness to Texas state government. And through our Leadership Circle program, the Comptroller's office is encouraging local governments throughout the state to follow suit and provide their constituents greater and easier access to their communities' financial and budgetary reports. These efforts build upon the strong Open Records/Freedom of Information laws we have in Texas that give our citizens the ability to monitor their government and hold it accountable. Informed citizens make our government stronger. We see that every day.

But when the public's right to know the business of its government threatens to reveal personally identifiable information, it creates a tension that must be acknowledged and addressed. It is the responsibility of government officials and concerned citizens alike to work together to strike the right balance between these competing concerns.

I am hopeful that this report will contribute to the discussion and lead to solutions that will keep Texas government open and transparent, while ensuring that our citizens' personally identifiable information is protected.

Sincerely,



Susan Combs

cc: The Honorable Rick Perry, Governor
The Honorable David Dewhurst, Lieutenant Governor
The Honorable Joseph R. Straus, III, Speaker of the House



Protecting Texans' Identities: The Challenges of Securing Privacy in Transparent Government
Table of Contents

Executive Summary	1
Chapter I: Introduction – Transparency vs. Privacy	4
Chapter II: Survey Methodology.....	8
Chapter III: Survey Results	11
Top 10 Pieces of Personally Identifiable Information Collected by State Agencies	12
Top 10 Pieces of Personally Identifiable Information Collected by Institutions of Higher Education	13
Frequency of Information Requests and Requesters.....	15
Chapter IV: Cost of Providing Information.....	17
Chapter V: Sale of Information under the Texas Transportation Code	29
Department of Public Safety	20
Department of Transportation	21
Department of Motor Vehicles	23
Parks and Wildlife Department.....	23
Chapter VI: Agencies’ and Institutions’ Views on Security of Information	25
Chapter VII: Public Information Law Trends in Texas and Nationwide	29
Public Information Law in Texas	29
Recent Texas Legislation.....	29
Attorney General Requests and Rulings	30
Nationwide Trends in Transparency	30
Nationwide Trends in Privacy Protection	31
Federal Legislation.....	32
Chapter VIII: Conclusion and Recommendations	33
Conclusion	33
Recommendations.....	34
Appendix A: Request Letter From Senator Duncan	
Appendix B: Types of Personally Identifiable Information Held by State Agencies and Public Institutions of Higher Education	
Appendix C: Forms and Documents Pertaining to the Sale and Disclosure of Information under the Texas Transportation Code	
Appendix D: Summary of Comments Obtained from Survey Participants	
Appendix E: Survey Instruments and Totals	
Appendix F: Fifty-State Comparison – Date of Birth	

Executive Summary: On Aug. 7, 2009, State Sen. Robert Duncan, Chair of the Senate Committee on State Affairs with jurisdiction over the Public Information Act, sent a letter to the Comptroller asking her office “to study, analyze and prepare a report on the amount and types of personally identifiable information collected by each state governmental body.” The analysis includes a study of the disclosure and sale of information contained in the state’s drivers license and motor vehicle records under Chapters 521, 522 and 730 of the Texas Transportation Code.

Chapter I outlines the challenges faced in maintaining a balance between protecting individual privacy rights and earning the public trust through transparency in government. On the one hand there is the growing concern with identity theft and protecting the massive quantity of personally identifiable information contained in databases maintained by state agencies and institutions of higher education. On the other hand is the need to show the public exactly what goes on as public officials conduct state business.

Texas is particularly sensitive to these competing issues. We have some of the strongest Open Records/Freedom of Information laws in the country, and our citizens appreciate this openness. However, Texas also has one of the highest identity theft complaint rates in the nation. According to a report published by the Federal Trade Commission in 2009, Texas had the third highest per capita identity theft complaint rate with 116 complaints per 100,000 people, behind only Florida (122) and Arizona (119). The report indicates that three South Texas metro areas (Laredo, McAllen, and Brownsville) lead the nation in per capita identity theft complaints.

Chapter II explains the project methodology. Six surveys were created and distributed to 62 public universities and 109 state agencies to capture:

- Bidder/Contractor Information
- Current and Former Personnel/Staff
- Information Security/Technology
- Clients/Students/Patients/Members
- Employment Applications
- Open Records

More than 2,000 survey responses were received, the majority from the “Clients /Students /Patients / Members” survey. Respondents were instructed to distribute copies to the heads of all pertinent programs for response. Consequently, many agencies submitted more than one survey for each category.

Chapter III summarizes the types and amounts of personally identifiable information collected and maintained by state agencies and institutions of higher education. The top five pieces of information collected as reported by state agencies and institutions of higher education are:

State Agencies	Occurrences	Institutions of Higher Education	Occurrences
First and Last Name	324,013,200	First and Last Name	36,374,764
Home Address	308,944,996	Date of Birth	31,877,230
Date of Birth	296,772,680	Phone (cell/home)	31,335,457
Social Security No.	229,217,021	Home Address	31,312,046
Medical Information	214,058,519	Personal e-mail address	30,260,854

Key Findings:

- As of Jan. 1, 2010, respondents reported that they have collected and stored more than **5 billion pieces of personally identifiable information.**

- Survey results show state agencies received more than 1 million written requests for information, with a large percentage including requests for personally identifiable information.
- Over the last five fiscal years, agencies have received approximately **\$324 million** for providing and selling information maintained in their systems.
- Agencies lack uniform procedures for handling and protecting personally identifiable information. While 81 percent of responding agencies and universities conduct frequent reviews of information security safeguards and approximately 19 percent conduct reviews infrequently (every other year or even less frequently), 14 percent indicated that they do not conduct any reviews.

Chapter IV discusses the total amount of monies received for providing any type of information, whether through open records cost recovery, subscription services or for providing information under the Transportation Code.

The Public Information Act gives the public the right to request information held by governmental entities while allowing agencies to recover costs, including materials, labor, and overhead, associated with providing copies of public information. A report on monies collected by state agencies for responding to open records requests is published by the Office of the Attorney General (OAG) and is available online on the OAG website. According to the OAG report, agencies collected approximately \$3.4 million over the fiscal 2008-09 biennium.

Based on our survey results, which cover more sources of funds than the above-mentioned report, agencies and institutions of higher education received approximately **\$133 million over the biennium**, most of which was received through the sale of information under the Transportation Code.

Chapter V deals specifically with the four agencies authorized to collect and sell data under the Transportation Code (Department of Public Safety, Department of Transportation, Department of Motor Vehicles and the Parks and Wildlife Department) and the circumstances under which they are allowed to do so. Over a five-year period (fiscal 2005-2009), the Department of Public Safety alone received over **\$284 million** for providing information under relevant provisions of the Transportation Code.

Chapter VI is an in-depth evaluation of the perceptions of agencies and universities as to the sufficiency of their methods for protecting personally identifiable information. Results indicate that most agencies and universities believe they sufficiently secure the collection, maintenance and transfer of personally identifiable information. Results indicate that 86 percent of agencies review safeguards (80 percent at least annually) but 14 percent never conduct reviews.

Survey results regarding training indicate:

- Only 67 percent of those responding to the open records questionnaire believe personnel receive adequate security awareness training. This may be consistent with the lower levels of awareness in this area, as only 26 percent of responses reported discussing personally identifiable information security weekly or monthly.
- While approximately 73 percent of responses to the Information Technology/Information Security instrument reported personnel receive adequate training, only 56 percent said they receive it annually.

Chapter VII provides an overview of transparency and personally identifiable information-related laws and legislation in Texas and around the country. National research shows states are taking steps to

improve transparency as they face whether and how to protect personally identifiable information that may be misused if publicly released or that may conflict with personal privacy interests.

Several states, including Texas, Arizona and Georgia, have taken steps to make public information more readily accessible for their citizens. Other states, including Illinois, Kansas, New Jersey, North Dakota and Nebraska, while also attempting to improve transparency and accessibility, have taken steps to exempt from public disclosure state employee personnel records with exceptions for such items as gross salary, employment history and employing agency. Other states have created information privacy and security committees to help improve the security of personal information collected by state and local government bodies.

Chapter VIII concludes the study with a series of recommendations based upon our findings, research and comments gleaned from the surveys, including the creation of an information security council or review board that should be responsible for:

- Creating statewide model training policies relating to the collection, handling and transfer of personally identifiable information;
- Reporting biennially to the Legislature on the status of privacy issues in Texas and making recommendations for changes to the Public Information Act in light of increased threat of fraud or identity theft or new technologies or situations affecting the privacy of Texans;
- Publishing a contact list for each agency for privacy and public information requests;
- Helping to decrease the amount of unnecessary personally identifiable information collected by governmental entities; and
- Improving agency employee awareness of the critical need for proper handling of personally identifiable information.

Chapter I: Introduction – Transparency vs. Privacy

Transparency in Government

Transparency in government is good public policy and good business. It allows citizens to know exactly what goes on when public officials transact public business. Local, state and federal governmental entities are taking steps to make their finances more visible and to show the public how state funds are spent. Comptroller Combs is committed to enhanced public access, from *Where the Money Goes* with drill-down tools to track state spending to TexasTransparency.org,¹ which provides public access to Comptroller data, more detailed information about state budget processes and spotlights on local government transparency efforts. As a result, the public is more engaged in how their hard-earned dollars are used, and helping government see where and how to save money and create efficiencies.

In addition, several state agencies are participating in the Enterprise Resource Planning (ERP) project, an effort called for by legislators during the 80th legislative session.² The goal of the state's ERP initiative, also called ProjectONE³ – Our New Enterprise, is to standardize and integrate financial, human resources and payroll applications across state agencies and institutions of higher education. This initiative will be a large step toward making each agency more transparent and accountable to taxpayers and enabling each agency to more easily track and manage its spending patterns.

Protecting Privacy

While government transparency is key to earning the trust of citizens, maintaining that trust may hinge on how well sensitive or confidential personally identifiable information is protected. Privacy issues sometimes find themselves on a collision course with the public's right to see the business of their governmental officials. Governmental agencies are holding billions of pieces of personally identifiable information about the citizenry, as well as similar information concerning various public employees, licensees, permit holders, contractors and others. This information, if obtained by a criminal element, could jeopardize the physical or financial safety of those individuals.

Texas is particularly sensitive to these competing issues. We have some of the strongest Open Records/Freedom of Information laws in the country. However, Texans are increasingly concerned about identity theft and acquisition of personally identifiable information by hackers and identity thieves.

Identity theft is the fastest growing white-collar crime in the United States.⁴ The Federal Trade Commission (FTC) estimates that 9 million individuals in the United States have their identities stolen every year.⁵ That is the equivalent of approximately 17 identities stolen *every minute*. Texas is certainly not immune to this nationwide crisis.

¹ www.texas Transparency.org/moneygoes/index.php

² Tex. H.B. 3106, 80th Leg., R.S. (2007)

³ See www.txprojectone.org/

⁴ See Tex. Attorney Gen. OR2006-09138 at 3; *Daly v. Metropolitan Life Ins. Co.*, 782 N.Y.S2d 530, 535-36 (N.Y. Sup. 2004); Federal Trade Commission, *FTC Consumer Alert; Privacy: Tips for Protecting Your Personal Information*, (Washington, D.C., August 2008), available at www.ftc.gov/bcp/edu/pubs/consumer/alerts/alt106.shtm. (Last visited July 18, 2010.);

⁵ Federal Trade Commission, *About Identity Theft*, (Washington, D.C.), available at www.ftc.gov/bcp/edu/microsites/idtheft/consumers/about-identity-theft.html (Last visited June 16, 2010.)

As Exhibit 1-1 demonstrates, Texas had the third highest per capita rate of identity theft complaints, with about 116 complaints per 100,000 people, behind only Florida (122) and Arizona (119).⁶

Exhibit 1-1
Top Five States by Number of Identity Theft Complaints
Per 100,000 Population

State	Complaints	Complaints Per 100,000
Florida	22,664	122.3
Arizona	7,875	119.4
Texas	28,844	116.4
California	42,209	114.2
Nevada	2,802	106.0

Source: Federal Trade Commission

Metropolitan areas in Texas were hit hard in 2009. Nine made the FTC's top 50 list of largest metropolitan areas for identity theft consumer complaints. The top three metropolitan areas for reported complaints of identity theft per 100,000 were in Texas (Exhibit 1-2), with Brownsville-Harlingen first.⁷

Exhibit 1-2
Top Ten Metropolitan Areas by Identity Theft Complaints
Per 100,000 Population

Metropolitan Area	Complaints	Complaints Per 100,000
Brownsville-Harlingen, TX	1,016	262.4
McAllen-Edinburg-Mission, TX	1,758	247.4
Laredo, TX	457	196.0
Miami-Fort Lauderdale, FL	10,457	193.2
Madera, CA	265	180.9
Dunn, NC	189	173.8
Merced, CA	424	172.7
Corpus Christi, TX	710	171.3
Greeley, CO	413	169.4
Bakersfield, CA	1,330	168.2

Source: Federal Trade Commission

Many of the complaints across Texas involve identity theft relating to information obtained through government documents or benefits.⁸ This makes sense as these types of institutions request a large amount of personally identifiable information from the public through employment applications, investigations, tax returns and other sources described in detail in the following chapters.

As this report will confirm, state agencies and public institutions of higher education in Texas are the repositories of staggering amounts of sensitive data, including Social Security numbers, dates of birth, addresses, personal e-mail addresses and credit histories. As hosts of this much sensitive data, state

⁶ Federal Trade Commission, *Consumer Sentinel Network Data Book for January - December 2009* (Washington, D.C., February 2010), p. 14, available at www.ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2009.pdf. (Last visited May 21, 2010.)

⁷ *Id.* at p. 16

⁸ *Id.* at p. 61 (indicating that 20 percent, or more than 5,700, of the complaints received in Texas related to this type of identity theft, second only to employment-related fraud)

agencies and universities are continually being attacked by hackers and other criminals, internal and external, looking to exploit any known vulnerability.

Information security experts predict that “more individuals will discover that they have become identity theft victims as they apply for government assistance and/or benefits. Not only will their own Social Security numbers be used, but they may be temporarily denied benefits due to the use of their child’s Social Security number, which has been used fraudulently. This type of identity theft...may be associated with complications with the IRS, Social Security Administration, Departments of Motor Vehicles, Medicare and Welfare.”⁹

Governmental entities in Texas are facing at least two significant challenges regarding personally identifiable information. First, as indicated in Exhibit 1-3, they have experienced significant information security incidents in the last five years, involving confidential or non-public information such as names linked to Social Security numbers, and the information may have been stolen, inadvertently disclosed to the public or otherwise compromised.

Exhibit 1-3
A Selected Sample of Recent Security Related Breaches
Texas State Agencies and Institutions of Higher Education

Date	Agency/Institution	Summary of Incident	Types of Records
19-Jul-07	Secretary of State	Names and Social Security numbers of thousands accessible on Texas Secretary of State website	SSN, names & addresses
16-Feb-08	Texas A&M University	Names and Social Security numbers of 3,000 inadvertently posted online	SSN, names & addresses
26-Apr-10	Texas Child Protective Services Division	Employee steals at least 70 adoptive and foster parents personal details	SSN, names & addresses
19-May-07	Texas Commission on Law Enforcement Officers Standards and Education	Social Security numbers, names, dates of birth of 229,000 on stolen computer	SSN, names & addresses, and dates of birth
31-May-06	Texas Guaranteed Student Loan Corporation	Third-party contractor lost a piece of equipment containing the names and Social Security numbers of about 1.3 million borrowers.	SSN, names & addresses
11-Sep-08	Texas Lottery Commission	Ex-employee was arrested for downloading Social Security numbers and names of lottery winners. A total of 89,000 records were affected.	SSN, names & addresses, account Info.
23-Apr-06	University of Texas - School of Business	Records including Social Security numbers breached for 197,000 people	SSN, names & addresses
4-Feb-10	University of Texas at El Paso	Mailing error exposes 15,000 students’ Social Security numbers in envelope window	SSN, names & addresses
5-Mar-10	University of Texas Southwestern Medical Center	12,000 patients exposed after a former employee was found in possession of a limited amount of patient billing data	Medical, dates of birth, financial

Source: *DataLossDB.org*

⁹ Robert Siciliano, *Top 10 Identity Theft Predictions for 2010*, <http://information-security-resources.com/2009/12/21/top-10-identity-theft-predictions-for-2010/>

It is clear that many security-related incidents in Texas involve the loss or theft of individuals' Social Security numbers, dates of birth and names and addresses, diminishing the public's trust.¹⁰

The second challenge facing governmental agencies is ensuring that individual privacy and legitimate financial and physical security concerns are adequately protected even in what may appear to be public records. For example, names, titles, and work addresses of public employees are deemed public information, but if an individual is a stalking or crime victim whose work location should be protected from disclosure, publishing this same information on the Internet could cause serious harm to that individual. The same may hold true for an individual who operates a home-based business.

In addition to the criminal and privacy implications, there are serious financial ramifications associated with this offense for businesses. The FTC reported losses to businesses and financial institutions of \$47.6 billion in 2002.¹¹ That figure has risen to approximately \$54 billion, according to a 2010 study conducted by Javelin Study & Research.¹²

As governments upload more public information to the Internet to provide greater public access and transparency, we will see a growing number of individual privacy interests and security issues affected. The Texas Attorney General's website provides resources to the public fight identity theft,¹³ including an identity theft victim toolkit which includes specific actions on how to monitor and stop ongoing damage to credit; how and where to report identity theft; how to prevent and curtail further identity theft abuses, and how to complete identity theft-related affidavits and declarations.¹⁴

Because of the severity of these issues, Sen. Robert Duncan, Chair of the State Affairs Committee, asked the Comptroller's office to study, analyze and prepare a report on the amount and types of personally identifiable information collected by each state governmental body, including a study of the disclosure and sale of this type of data under Chapters 521, 522, and 730 of the Texas Transportation Code.¹⁵

The remaining chapters in this report provide more detail on the methodology of the study, the amount and types of personally identifiable information collected by state agencies, sharing and disclosure of personally identifiable information generally and under the Transportation Code, safety and security of personally identifiable information, recent legislation and opinions impacting Texas and other states around the country, and a list of recommendations for legislation and the possible effects of the recommendations.

¹⁰ This is consistent with nationwide data presented by DataLossDB.org, which provides a breakdown of events (by data type) involving the loss, theft or exposure of PII that have occurred since 2001. According to Datalossdb.org, 34 percent of the incidents involved name and address, 31 percent involved Social Security number, and 7 percent related to dates of birth.

¹¹ Federal Trade Commission, *Identity Theft Survey Report*, (Washington, D.C., September 2003), p.7, available at www.ftc.gov/bcp/edu/microsites/idtheft/downloads/synovate_report.pdf. (Last visited July 22, 2010.)

¹² Javelin Strategy & Research, *2010 Identity Fraud Survey Report: Identity Fraud Continues to Rise – New Accounts Fraud Drives Increase; Consumer Costs at an All-Time Low*, (Pleasanton, CA, February 2010), p.8, available at www.javelinstrategy.com/uploads/files/1004.R_2010IdentityFraudSurveySampleReport.pdf (Last visited July 27, 2010.)

¹³ Texas Office of the Attorney General, *Fighting Identity Theft*, www.texasfightsidtheft.gov/

¹⁴ Texas Office of the Attorney General, *Identity Theft Victim's Kit*, www.texasfightsidtheft.gov/pdfs/IDTheft_kit.pdf

¹⁵ Letter from Robert Duncan, State Senator, to Susan Combs, Comptroller of Public Accounts (Aug. 7, 2009)

Chapter II: Survey Methodology

In October 2009 a letter was mailed to all state agencies and public institutions of higher education explaining the purpose and scope of the study and requesting participation. As a first step, participants were asked to identify and assign a contact person to work closely with the CPA Personally Identifiable Information project team. Six surveys were then developed to determine the volume and nature of personally identifiable information within targeted departments of participating entities. By February 2010 rough drafts of the six surveys¹⁶ were created to collect information on:

- Contractors/bidders/proposers.
- Agency/institution current and former employees.
- Employment applications.
- Information technology/information security.
- Open Records division.
- Clients, students, and service recipients.

Throughout March and April 2010, three strategies were implemented to improve the validity and reliability of the surveys. First, face validation of the surveys was conducted by the project group and selected staff members within the Comptrollers' office with expertise in specific areas. Second, the surveys were assessed and reviewed by a selected group of Comptroller staff with expertise in the respective fields. For example, the Employee Survey was assessed by those with expertise in human resources policies and procedures, while the IS/IT survey was assessed by those in data collection, computer security and technology. Third, selected agencies/institutions were sent pilot questionnaires to assess the clarity of the questions and the availability of the requested data. Comments received through these strategies were incorporated to enhance the validity and reliability of the surveys.

In May 2010 the instruments were e-mailed to all designated individuals within the state agencies and institutions of higher education along with a copy of Sen. Duncan's letter¹⁷ and a step-by-step set of instructions. The agencies were given two weeks to return completed surveys. It is imperative to note that while a two-week timeframe was set for data collection, the actual data collection took more than four months due to requests for extensions, clarifications, follow up and validation of submitted information. All six surveys were e-mailed to the state agencies and institutions of higher education listed in Exhibit 2-1.

To include all potential divisions, sections and departments within the participating agencies, which collect, store or work with personally identifiable information, the designated contacts were instructed to disseminate the instruments to all relevant departments. For instance, entities having relevant programs within a survey category were instructed to disseminate surveys to the heads of all relevant programs for response. We collected 2,048 completed and usable surveys from 109 state agencies and 62 institutions of higher education.

- Contractors/bidders/proposers – 189 surveys
- Current and former employees – 170 surveys
- Employment applications – 173 surveys
- Information technology/information security – 175 surveys
- Open records – 191 surveys
- Clients, students and service recipients – 1,150 surveys

¹⁶ Copies of the surveys and results are included in Appendix E

¹⁷ See Appendix A

Exhibit 2-1
List of all Public Institutions of Higher Education
in Texas Included in this Report

Angelo State University	Texas A&M University - San Antonio	Texas State University - San Marcos	University of Texas at Austin
Lamar Institute of Technology	Texas A&M University (College Station)	Texas Tech University	University of Texas at Brownsville
Lamar State College - Orange	Texas A&M University at Galveston	Texas Tech University/System	University of Texas at Dallas
Lamar State College - Port Arthur	Texas A&M Agrilife Extension	Texas Transportation Institute	University of Texas at El Paso
Lamar University - Beaumont	Texas A&M Agrilife Research	Texas Woman's University	University of Texas at San Antonio
Midwestern State University	Texas A&M Health Science Center	The Texas A&M University System	University of Texas at Tyler
Prairie View A&M University	Texas A&M University - Central Texas	Texas Engineering Experiment Station	University of Texas System
Sam Houston State University	Texas A&M University- Texarkana	Texas State University System Board of Regents	UNT Health Science Center - Fort Worth
Stephen F Austin State University	Texas Engineering Extension Service	Texas Tech University Health Sciences Center	UT Health Science Center - Houston
Sul Ross State University	Texas Forest Service	University of Texas - Permian Basin	UT Health Science Center - San Antonio
University of Texas at Arlington	Texas Southern University	University of Houston - Victoria	UT MD Anderson Cancer Center
Tarleton State University	Texas State Technical College	University of Houston/ System	UT Medical Branch at Galveston
Texas A&M International University	University of Texas Health Center at Tyler	University of North Texas	UT Southwestern Medical Center - Dallas
Texas A&M University - Corpus Christi	University of Houston	University of North Texas/System Admin.	West Texas A&M University
Texas A&M University - Commerce	University of Houston - Clear Lake	University of Texas – Pan American	University of Houston - Downtown
Texas A&M University - Kingsville			

Exhibit 2-2
List of all Texas State Agencies Included in the Report

Adjutant General	Alcoholic Beverage Commission	Appellate Courts	Board of Chiropractic Examiners
Board of Examiners of Psychologists	Board of Nurse Examiners	Board of Plumbing Examiners	Board of Tax Professional Examiners
Board of Veterinary Medical Examiners	Brazos River Authority	Cancer Prevention and Research	Commission/State Emergency Communication
Commission on Jail Standards	Commission on Uniform State Laws	Consumer Credit Commissioner	Credit Union Department
Department of Agriculture	Department of Banking	Department of Public Safety	Department of State Health Services
Department of Family and Protective Services	Department of Aging and Disability Services	Department of Assistive and Rehabilitative Services	Department of Licensing & Regulation
Department of Savings and Mortgage Lending	Employees Retirement System	Executive Council of Physical and Occupational Therapy	Fire Fighters Pension Commission
Guadalupe-Blanco River Authority	Health and Human Services Commission	Health Professions Council	Legislative Budget Board
Legislative Reference Library	Lower Colorado River Authority	Office of Court Administration	Office of Injured Employee Counsel
Office of Public Insurance Counsel	Office of Public Utility Counsel	Office of Rural Community Affairs	Office of State Prosecuting Attorney
Parks and Wildlife Department	Public Utility Commission of Texas	Railroad Commission	Real Estate Commission
Texas School for the Deaf	Texas School for the Blind and Visually Impaired	Soil & Water Conservation Board	State Bar of Texas
State Board of Public Accountancy	State Energy Conservation Office	State Office of Administrative Hearings	State Office of Risk Management
State Pension Review Board	State Preservation Board	Office of State-Federal Relations	Sunset Advisory Commission
Teacher Retirement System	Texas Animal Health Commission	Texas Board of Land Surveying	Texas Board of Law Examiners
Texas Board of Prof. Engineers	Texas Board of Professional Geoscientists	Texas Bond Review Board	Texas Commission on Environmental Quality
Texas Commission on Law Enforcement	Texas Commission on the Arts	Texas Department of Insurance	Texas Department of Transportation
Texas Department of Criminal Justice	Texas Education Agency	Texas Ethics Commission	Texas Funeral Service Commission
Texas Historical Commission	Texas Juvenile Probation Commission	Texas Legislative Council	Texas Lottery Commission
Texas Medical Board	Texas Optometry Board	Texas Public Finance Authority	Texas Racing Commission
Texas State Board of Pharmacy	Texas Veterans Commission	Texas Water Development Board	Texas Youth Commission
Texas Board of Architectural Examiners	Texas Commission of Fire Protection	Texas Dept. of Housing and Community Affairs	Texas Higher Education Coordinating Board
Board of Dental Examiners	Residential Construction Commission	Texas Facilities Commission	State Securities Board
General Land Office	State Law Library	Texas State Library & Archives Commission	Department of Information Resources
Texas Structural Pest Control Board	Office of the Attorney General	Secretary of State	Texas Workforce Commission
Commission on Judicial Conduct	Comptroller of Public Accounts	State Auditor's Office	Texas County & District Retirement System
Texas State Board of Podiatric Medical Examiners	Texas Veterinary Medical Diagnostic Laboratory	Trinity River Authority	Sabine River Authority
OneStar Foundation			

Part III: Survey Results

Number and Types of Personally Identifiable Information:

In each survey, participating agencies and institutions were asked to identify the types of personally identifiable information collected by their divisions. An exhaustive list of all possible personally identifiable information items was included. The respondents were simply asked to check those that their entity collects. A few other¹⁸ categories were provided to capture items not included in that list.

Exhibit 3-1 shows the list of personally identifiable information items included.

Exhibit 3-1
Itemized Personally Identifiable Information

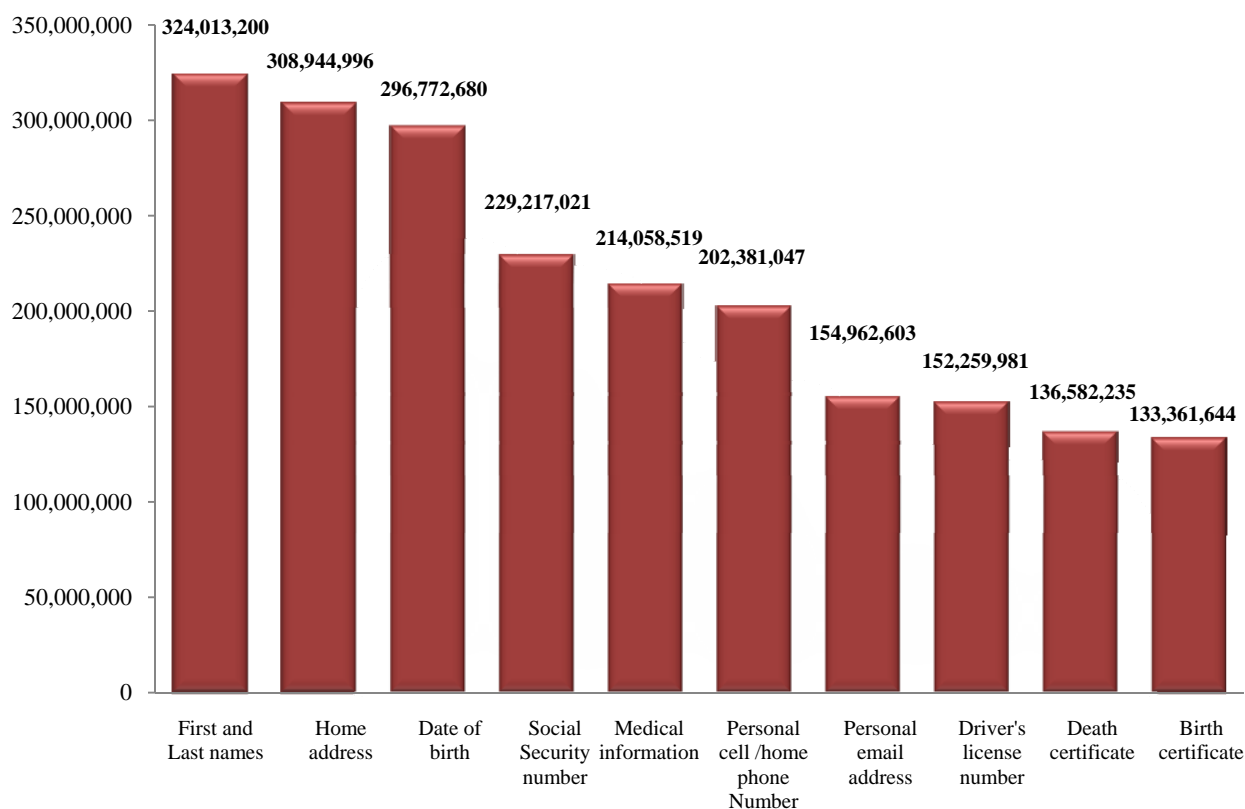
Account number login information	Accounting records	Background/reference information	Banking information
Bid/contract/consultation amount	Birth certificate	Birthplace	Bond information
Business capacity information	Business insurance information	Business/personal financial statements	Contract/bid/consultation history
Credit card/debit card number	Credit history	Criminal record	Customer list
Date of birth	Death certificate	Divorce decree	Drivers license number
Educational background	Emergency contact information	Employment date	Federal employment ID number
Federal income tax information	Fingerprints	First and last name	Handwriting sample
Home address	Immigration/naturalization status	Info about employee's child(ren)	Info about employee's spouse
Lien information	Loan information	Medical information	Mother's maiden name
Motor vehicle information	Name of employees	Name/information about previous business owner	Outside employment
Passport number	Personal cell/home phone number	Personal e-mail address	Photo
Physically impaired information	Previous contracts	Performance evaluations	Qualification information
Reference check	Retina or iris image	Social Security number	Substance abuse related information
Tax preparer information	Tax violations	Texas taxpayer ID	Will
Work phone number	Other		

¹⁸ Some of the items described in the “other” category include the following: Texas and national Medicaid provider identification number, Texas Bar card number, number in household, marriage license, high school transcript, sex offender status and primary language.

Top ten pieces of PII collected by State Agencies:

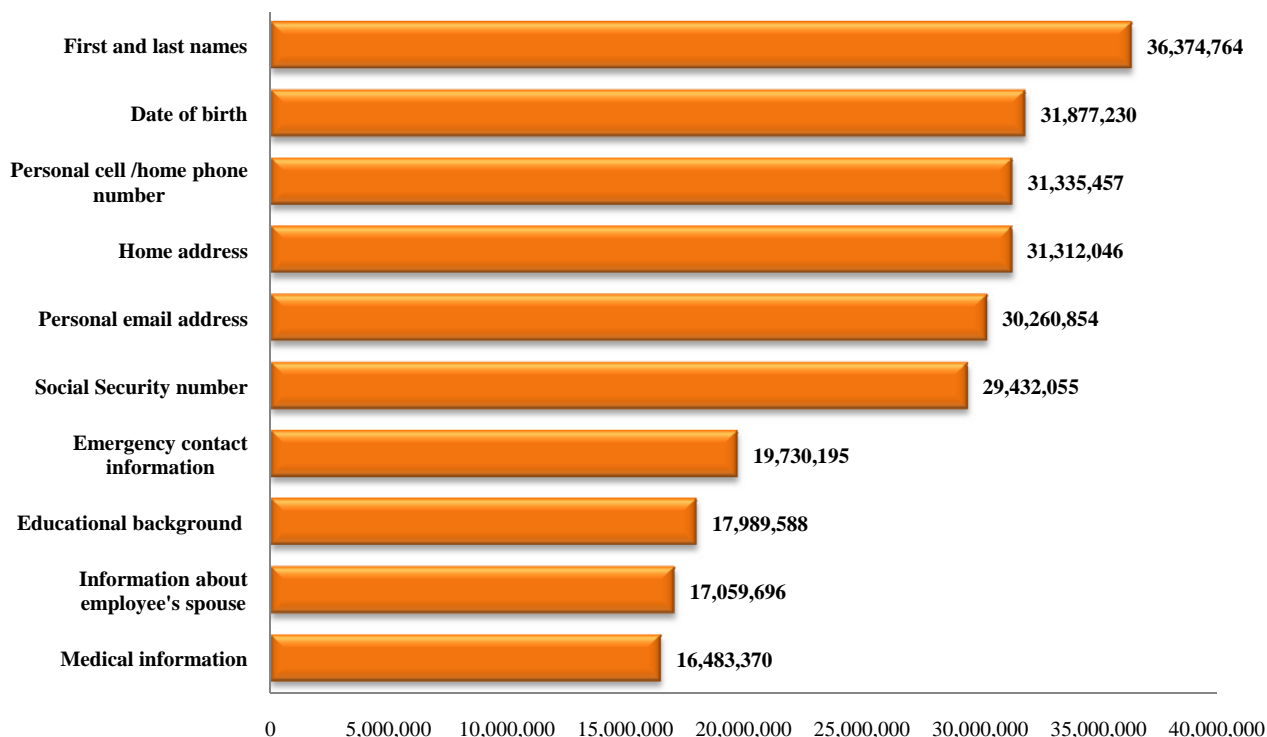
First and last names were most frequently collected and maintained by state agencies (Exhibit 3-2). Home address was the second most collected piece of information, followed by date of birth and Social Security number. The total number of items collected in each category reflects those that state agencies collect from current/former employees, employment applicants, service recipients, members, clients and bidders/contractors/consultants. Collection of Social Security numbers was less frequent than the first and last names due to that fact that personally identifiable information collected from members/service recipients (i.e., university gym members, outreach and continuing education program participants, conference attendees, etc.) was usually limited to name, home address and date of birth.

Exhibit 3-2
Top 10 Pieces of Personally Identifiable Information
Collected and Maintained by State Agencies

***Top 10 Pieces of Personally Identifiable Information collected by Institutions of Higher Education:***

The same trend was noted in reference to personally identifiable information collected by the institutions of higher education. First and last names were the most frequently collected types of personally identifiable information. Date of birth, personal cell/home telephone number and home address were the second, third, and fourth most collected items, respectively (Exhibit 3-3).

Exhibit 3-3
Top 10 Pieces of Personally Identifiable Information
Collected and Maintained at Institutions of Higher Education



A comparison between the top 10 personally identifiable information items collected by the state agencies and institutions of higher learning shows a different pattern and frequency of data collection. For example, “home address” and “Social Security number” appeared higher in the top 10 list for the state agencies while “personal cell/home phone number” appeared higher on the institutions’ top 10.

Total Number of Personally Identifiable Information Items Collected by State Agencies and Institutions of Higher Education

Exhibit 3-4 shows the total number of personally identifiable information items collected and stored by all participating state agencies and institutions of higher education. ***More than 5 billion pieces of personally identifiable information*** were collected and stored in various databases as of Jan. 1, 2010. Six potential sources of personally identifiable information within state agencies and institutions of higher education:

1. **Membership List:** Several agencies and institutions of higher education have created databases containing members, customers, licensed individuals and certified businesses.
2. **Client and service recipients:** Many agencies and institutions of higher education (medical and health science centers) have exhaustive lists of individuals who directly or indirectly receive social, financial and medical services.
3. **Current and former students:** This category lists all current and former students from the institutions of higher education. Only a few state agencies indicated collection of personally identifiable information regarding students (Attachment B).

4. **Current and former employees:** This category reflects the number of current and former employees as of Jan. 1, 2010.
5. **Employment applicants:** The amount of personally identifiable information in this category is based on the number of employment applications received by the state agencies and institutions of higher education during fiscal 2009 only.
6. **Contractors/bidders/consultants:** This category reflects personally identifiable information collected through submission of bids and proposals by potential bidders, proposers, consultants and contractors.

Exhibit 3-4 in Appendix B shows that the largest amount of personally identifiable information collected by state agencies and institutions of higher education was related to individuals who directly or indirectly received social, financial or medical services (86 percent). Here are a few examples of those classified as clients or service recipients:

- Individuals receiving medical services from various medical and health science centers
- Individuals receiving from Health and Human Services agencies or their components direct or indirect services such as mental health programs, substance abuse treatment, etc.
- People receiving financial benefits such as unemployment or recipients of services relating to the Texas Tomorrow Fund, Texas Tuition Promise Fund, Unclaimed Property, etc.

The “current and former students” category generated the second largest amount of personally identifiable information collected by the institutions of higher education, followed by the “members list” created by state agencies and institutions of higher education. The lowest number of personally identifiable information items collected belonged to bidders, proposers, consultants and contractors which accounted for nearly 85.5 million personally identifiable information items.

Among all pieces of personally identifiable information collected, first and last names (360,387,964) were the most frequently collected, followed by home address (340,257,042). Based on the present Texas population¹⁹ (24 million), on average each citizen’s name and address is stored in the records or databases of at least 15 state agencies or institutions of higher education.

Also highly collected were dates of birth (329 million), Social Security number (259 million), personal cell/home phone numbers (234 million) and medical information (231 million). Other items collected include 38 million fingerprints, more than 54 million photos, nearly 55 million passport numbers and more than 59 million items related to federal income taxes.

In addition to a detailed list of all personally identifiable information items (Exhibit 3-4), several statistical tables are included in Appendix B depicting:

- 1) Personally identifiable information collected by State Agencies versus Institutions of Higher Education (Exhibit B-1).
- 2) Volume and percentage of personally identifiable information collected through employment applications submitted to state agencies and institutions of higher education (Exhibit B-2).
- 3) Personally identifiable information collected by both groups from students, clients and service recipients (Exhibit B-3).
- 4) Amount of personally identifiable information collected from potential bidders, contractors and consultants (Exhibit B-4).

¹⁹Texas State Data Center and Office of the State Demographer, *2007 Total Population Estimates for Texas Places* (Estimates of the total populations of counties and places in Texas for July 1, 2007 and Jan. 1, 2008), (produced by the Institute for Demographic and Socioeconomic Research, University of Texas at San Antonio, October 2008), available at http://txsdc.utsa.edu/tpepp/2007_txpopest_place.php.

Frequency of Information Requests and Requesters: A summary of open records requests and their referral to the Office of the Attorney General (OAG) from fiscal 2009 is presented in Exhibit 3-5. State agencies and institutions of higher education received 1,070,991 open records requests.²⁰ Of those requests, more than 99 percent were received by state agencies and less than 1 percent by institutions of higher education.

Of the requests, 712,293 (66.5 percent) asked for personally identifiable information. More than 99 percent of those open records requests were to state agencies.

Exhibit 3-5 also shows the number and percentage of personally identifiable information-related requests referred to the OAG for ruling. As shown in the exhibit, less than 1 percent of personally identifiable information-related requests are referred to the OAG from state agencies. Institutions of higher education referred personally identifiable information-related requests to the OAG more frequently than state agencies. A majority of the personally identifiable information-related requests referred to the OAG in fiscal 2009 (1,118 out of 1,247 requests, nearly 90 percent) were ruled to be protected from disclosure.

Exhibit 3-5
Number of Open Records Requests and the Proportion Referred to the Office of Attorney General

Requests		State Agencies		Institutions of Higher Education		Total
		Number	Percent	Number	Percent	
All Requests In Fiscal 2009		1,064,652	99.4%	6,339	0.6%	1,070,991
	Personally Identifiable Information-Related Requests	708,656	99.5%	3,637	0.5%	712,293
Personally Identifiable Information-Related Requests Referred to OAG		917	73.5%	330	26.5%	1,247
	Of those Referred to OAG, How many Ruled to be Protected	849	75.9%	269	24.1%	1,118

We asked the Open Records administrators to rank the source of requests for personally identifiable information, using the following categories: Individuals, Legislature, Media and Businesses. Requests outside those categories were grouped under the “other” category. The respondents were asked to rank those options based on the number and frequency of requests. The results are presented in Exhibit 3-6.

²⁰ This number varies from the 2,397,821 figure reported to the Office of the Attorney General (OAG), (*at* www.oag.state.tx.us/open/pia/reports/requests_tally.php?fy=2009&ag=all), as some agencies participating in the underlying study either did not report amounts to the OAG website at all or reported different amounts to the OAG website than they did for this study.

Exhibit 3-6
Ranking of Requesters for Personally Identifiable Information

Requester	Rank
Individuals	1st
Businesses	2nd
Media	3rd
Legislators	4th
Other	5th

The “other” category reflected personally identifiable information data requests from state government agencies, federal government agencies, city/county departments and attorneys.

Chapter IV: The Cost of Providing Information

The Texas Public Information Act gives the public the right to request information held by governmental entities, and allows agencies to recover some costs, including materials, labor and overhead, associated with providing copies of public information.²¹ Respondents were asked whether their agency/institution receives revenue through the cost recovery process or from other sources for providing information (Exhibit 4-1). More than three-quarters of respondents indicated that their agency/institution receives at least some revenue for providing information. Only 24.1 percent (39 agencies/institutions) stated that they do not receive revenue for sharing information.

Exhibit 4-1

Does Agency/Institution Recover the Costs of Providing Information?

Response	Number	Percent
Yes	122	75.3%
No	39	24.1%
No Response	1	0.6%
Total	162	100.0%

Those who provided an affirmative response to that question were asked to provide dollar amounts received from fiscal 2007 through fiscal 2009. The intention here was to account for all revenue received for providing information (i.e. cost recovery, subscription services, sale of data under the Transportation Code, etc.). Exhibit 4-2 shows that state agencies and institutions of higher education received an average of \$64,895,809 per year during fiscal 2005 through fiscal 2009 for cost recovery. Exhibit 4-2 also shows that over 99 percent of the aforementioned funds were received by state agencies.

Exhibit 4-2

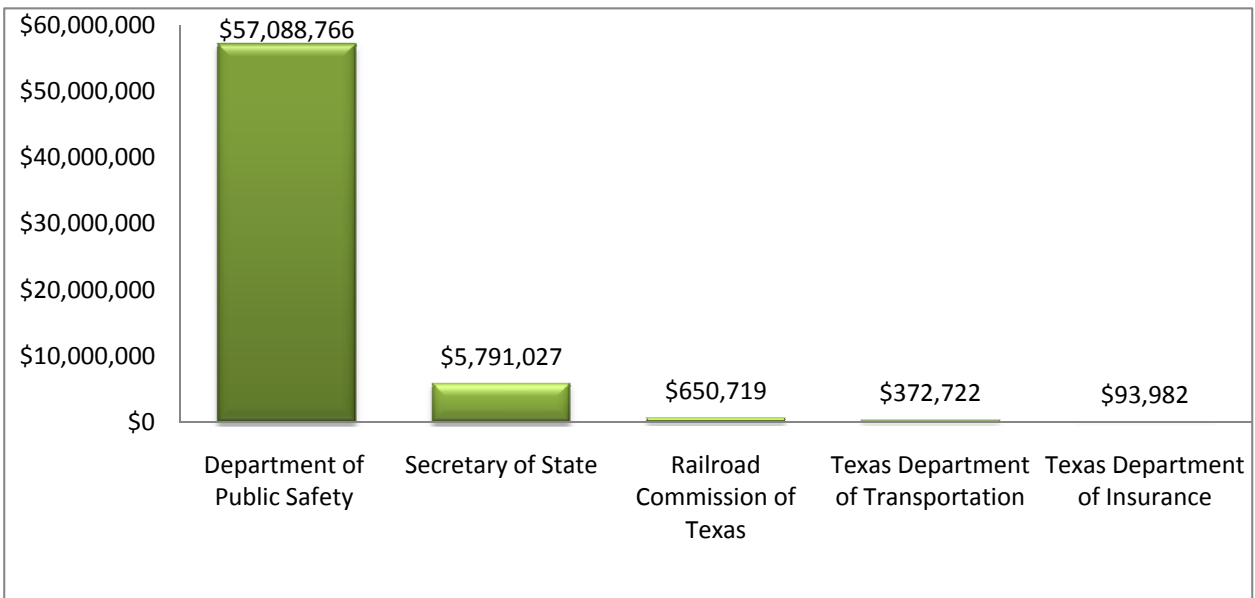
Amounts Received for Providing all Types of Information By Fiscal Year

Fiscal Year	State Agencies		Institutions of Higher Education		Total
	Amount	Percent	Amount	Percent	
2005	\$60,852,440	99.9%	\$38,378	0.1%	\$60,890,818
2006	\$65,254,609	99.9%	\$45,605	0.1%	\$65,300,214
2007	\$66,053,038	99.9%	\$48,053	0.1%	\$66,101,091
2008	\$66,601,491	99.9%	\$54,093	0.1%	\$66,655,584
2009	\$65,486,151	99.9%	\$45,189	0.1%	\$65,531,340
5-Year Total	\$324,247,729	99.9%	\$231,318	0.1%	\$324,479,047

²¹ Tex. Gov't Code Ann. § 552.261; *See also*, 1 Tex. Admin. Code §§ 70.3, 70.4; and 37 Tex. Admin. Code § 405.5.

Exhibit 4-3 depicts the top five agencies receiving funds for providing all types of information, including information provided through subscription services, through cost recovery under the Public Information Act, and by sale via the Transportation Code during fiscal 2009. As the exhibit reflects, the Texas Department of Public Safety (DPS) led all agencies, receiving close to 90 percent of the total revenue received by all state agencies and institutions of higher education during that period (\$57,088,766). The Secretary of State's office was second (\$5,791,027) followed by the Texas Railroad Commission (\$650,719). The next chapter explains the DPS figures in more detail.

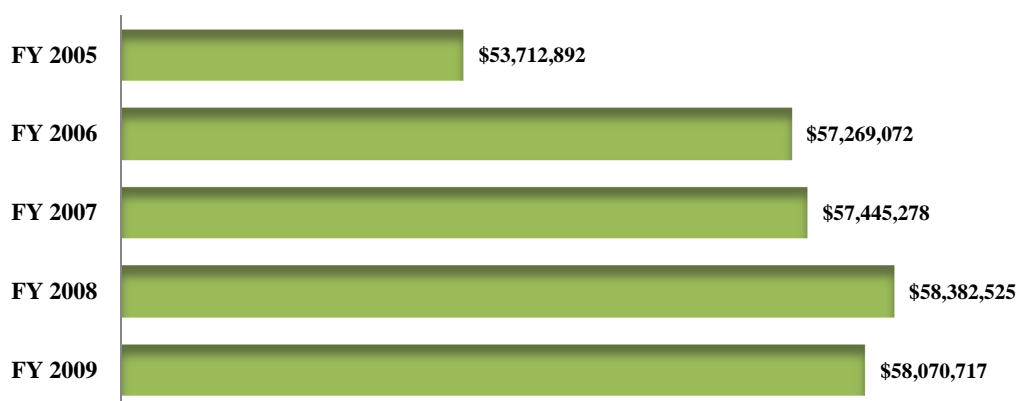
Exhibit 4-3
Top Five Agencies in Funds Received for Disseminating and/or Selling Information
Average Annual Revenue During Fiscal 2005 through Fiscal 2009



Part V: Sale of Information under the Texas Transportation Code

Four agencies may release information under the Transportation Code: The Department of Public Safety (DPS), Department of Transportation (TxDOT), Department of Motor Vehicles (DMV) and the Parks and Wildlife Department (TPWD). The table below reflects the total revenue for fiscal years 2005 through 2009, relating to the sale of information under the Transportation Code, as reported by the above agencies.

Exhibit 5-1
Total Revenue Received through Sale of Information under the Transportation Code
By Fiscal Year



In total, the four agencies have received more than \$284 million over the five-year period. Most of this revenue is received by DPS.

The remainder of this chapter will review the roles of the four agencies in the collection and sale of personally identifiable information contained within drivers license and motor vehicle-related databases.²²

I. Department of Public Safety:

DPS²³ compiles and maintains certain public information, such as agency investigations, arrests, violations, citations, convictions, accidents, motor vehicle title and registration and drivers license records.²⁴ Upon proper request, eligibility and authorization, DPS provides the public with copies of these records. [See *Appendix C* for a sample of the current Form] Additionally, DPS employees perform services related to this collected information, such as providing copies and performing National Driver

²² See *Appendix C* for a history of the privacy protection provisions in the Texas Transportation Code and a brief review of the relevant statutes

²³ DPS participants included the Driver License Division, responsible for maintaining the integrity of the Texas driver license, traffic safety through the examination and licensing of drivers, the improvement and control of problem drivers, revoking licenses and traffic and criminal law enforcement; and a grouping of other divisions, including human resources management, facilities management, administrative services, procurement and contract management, fleet operations and training and recruiting; and, the processing of “non-driver’s license related” records and requests, such as employee background checks; *Also see*, Texas Department of Public Safety, *Window on Compact with Texans*, www.txdps.state.tx.us/compact/

²⁴ 37 Tex. Admin. Code, § 1 (Tx. Dept. of Public Safety); *See also* Tex. Trans. Code Ann. § 730

Register (NDR) searches on behalf of current or prospective employers of individuals seeking employment as operators of commercial motor vehicles or railways.²⁵

Each of the program areas collects, maintains and potentially releases personally identifiable information. For instance, certain information from a driver's record may be purchased from DPS for a fee set by the State Legislature and agency rules. The table below summarizes the types of data sold and the current fee²⁶ structure:

Record Type	Record Description	Use and/or Requestor	Fee
1	Individual records and status check. Includes Name, DOB, License, and Last known address.	Used to determine whether an individual has a license or to obtain the licensee's last known address.	\$4 (\$6 for certified copy) ²⁷
2/2a	Three-year driving history. Includes name, DOB, license status, accidents where citation issued and moving violations. 2a is the certified version.	Often used by employers to check driving record. Employer's check of commercial drivers' driving records is required annually by the U.S. Dept. of Transportation.	\$6 (\$10 for certified copy)
3/3a	List of all crashes and violations in driving record. Includes name, DOB, license status, list of crashes and violations. 3a is the certified version	May be requested by license holder or by any person eligible to receive the info. under Chapter 730, Transportation Code, if the licensee holds a commercial license. Often used as proof of completing driver safety course for dismissal of certain traffic violations.	\$7 (\$10 for certified copy)
	Certified Abstract of complete driving record	May be obtained by governmental entities, entities assisting governments for use in conjunction with a court or administrative proceeding, an employer, agent or insurer or, if licensee holds a commercial license, by any person eligible to receive the information under Chapter 730	\$20
4a	School bus records	Public schools and school districts request when checking driving record of those driving buses	Free
	Bulk Files containing names, addresses, and DOB of all license and identification certificate holders (21 million) in DPS' basic drivers license record file. ²⁸	Purchasers must sign agreement and certify in writing that they are eligible to receive the information under Chapter 730.	\$2,000 and \$75 for each weekly update ²⁹

Source: Department of Public Safety

Unlike the Texas Public Information Act, which prohibits a governmental body from inquiring into a requestor's reasons or motives for requesting information,³⁰ the Transportation Code *requires* the purchasers of drivers license data to execute a form that certifies their use of the information to be for one of the permissible purposes defined in the statute.³¹ Examples of "permissible purposes" are limited to

²⁵ Tex. Transp. Code Ann. § 521.056

²⁶ Some Records may be purchased via the state website found at www.texas.gov. The fees assessed for these records include an online administrative fee

²⁷ Tex. Transp. Code Ann. §§ 521.045 - .0475

²⁸ *Id.* § 521.050

²⁹ *Id.* § 521.052

³⁰ Tex. Gov't Code Ann. §§ 552.222 - .223

³¹ Tex. Transp. Code Ann. §§ 730.007, .012; *See also* 37 Tex. Admin. Code §§ 15.142, .144 (Texas Department of Public Safety)

such things as law enforcement actions, establishing identity and screening individuals for employment purposes.

The Drivers License Division received 11,519,788 requests. The annual revenue from fees collected for providing these records and related services, reported for purposes of this study by DPS, are reflected in the table below. Note: “PIA” represents amounts received for complying with open record requests under the Public Information Act (PIA).

Exhibit 5-2
DPS Revenue from Release of Information
Under PIA & Transportation Code

Fiscal Year	PIA ³²	Drivers License (under Transp. Code)	TOTAL Income
2005	\$ 375,141	\$ 53,712,892	\$ 54,088,033
2006	\$ 345,613	\$ 57,269,072	\$ 57,614,685
2007	\$ 381,810	\$ 57,445,278	\$ 57,827,088
2008	\$ 65,666	\$ 58,055,103	\$ 58,120,769
2009	\$ 52,723	\$ 57,740,532	\$ 57,793,255
Totals	\$1,220,953	\$ 284,222,877	\$ 285,443,830

DPS indicated that monies received for providing driver records and information are deposited to the Texas Mobility Fund, Comptroller Fund 00365, which by definition is to be used for construction and reconstruction of state highways. These funds are not appropriated to DPS.

II. Department of Transportation

The Texas Department of Transportation (TxDOT) is the official repository for all operator and officer-generated motor vehicle accident reports, known as the “Texas Peace Officer’s Crash Report,” and all reports of medical examiners and justices of the peace prepared to record a motor vehicle accident fatality.³³ That function was transferred from DPS to TxDOT’s *Traffic Operations Division* by the 80th Texas Legislature, Senate Bill 766, effective Oct. 1, 2007.³⁴ This accident information is maintained in a database referred to as the Crash Records Information System (CRIS).³⁵ TxDOT tabulates and analyzes the vehicle accident reports it receives and publishes statistical information at least annually³⁶ and also provides DPS with electronic access to the system.

The crash reports contain personal information such as names, addresses, drivers license numbers, vehicle identification numbers, proof of financial responsibility (insurance), medical information and citation data. [See *Appendix C* for a sample of the current form.] Additional information, such as the location of the accident, road conditions at the time of the crash, investigator’s opinion of what happened in the crash (which may include an investigation of possible causes) may be included in the report.

³² Prior to fiscal 2008, DPS was the official repository for the official “Peace Officer’s Crash Report” forms. The legislature shifted this function over to TxDOT beginning Oct. 1, 2007 (fiscal 2008).

³³ 43 Tex. Admin. Code § 1 (Tx. Dept. of Transportation – Traffic Operations – Crash Records Information System); see also Tex. Transp. Code Ann. §§ 521, 522, 550 and 730

³⁴ Tex. S.B. 766, 80th Leg., R.S., (2007)

³⁵ 43 Tex. Admin. Code §25.971 (Tx. Dept. of Transportation - Crash Records Information System)

³⁶ Tex. Transp. Code Ann. §201.806 (Acts 2009, 81st Leg., R.S., Ch. 522, Sec. 1, Sept. 1, 2009)

During the 81st Texas Legislature, Senate Bill 375 was passed (effective June 19, 2009) amending the Transportation Code to provide that all information related to a report of a motor vehicle accident that is maintained by TxDOT or any other governmental entity is privileged and for confidential use of TxDOT and agencies of the federal government, this state or a local government of this state that has use for the information for accident prevention purposes only.³⁷ Upon written request and payment of any required fees, TxDOT, or the governmental entity authorized to receive this data, may release the information to:

- (1) the law enforcement agency that employs the peace officer who investigated the accident and prepared the accident report;
- (2) the court in which a case involving a person involved in the accident is pending, if report is subpoenaed; or
- (3) a person who provides two or more of the following (**also known as the “2 of 3” requirement**):
 - (a) date of the accident,
 - (b) specific address or the highway or street where the accident occurred, or
 - (c) name of any person involved in the accident.³⁸

The statute also requires the fee that may be charged for the information to be calculated in the manner specified by the Public Information Act for public information provided by a governmental body. Currently, the fee for a copy of the accident report is \$6. The copy may be certified for an additional \$2. For a \$6 fee, TxDOT may issue a certification that no report or information is on file.³⁹ [See *Appendix C* for a sample of the current form].

Unless a requester can qualify under the “2 of 3” requirement referenced above, TxDOT is required to *withhold* or *redact* certain pieces of information when releasing this accident information in aggregate, including but not limited to the following pieces of information: name of any person, drivers license number, date of birth (other than the year), address (other than the ZIP code) and telephone number.⁴⁰

The number of requests received and the fees collected for providing these records for the last three fiscal years as reported by TxDOT is reflected in Exhibit 5-3.

Exhibit 5-3
TxDOT Number of Requests and Revenue for
Release of Motor Vehicle Accident Information from
Crash Records Information System (CRIS) Database
(Fiscal 2008-10)⁴¹

Fiscal Year⁴²	# Requests	CRIS Revenue
2008	25,672	\$ 327,422
2009	25,121	\$ 330,185
2010	25,966	\$ 332,167
Totals	76,759	\$ 989,774

³⁷ Tex. S.B. 375, 81st Leg., R.S., (2009); *See also* Tex. Trans. Code Ann. §550.065

³⁸ Tex. Trans. Code Ann. §550.065(c)

³⁹ *Id.* at (d)

⁴⁰ *Id.* at (f)

⁴¹ These figures reflect number of requests and fees collected for fiscal 2010 through Aug. 20, 2010.

⁴² The Legislature shifted this function from DPS to TxDOT beginning Oct. 1, 2007 (fiscal 2008).

III. Department of Motor Vehicles

The 81st Texas Legislature passed House Bill 3097 amending the Transportation Code and creating the Department of Motor Vehicles (DMV) as a separate agency responsible for drivers and their vehicles.⁴³

Certain information contained in the vehicle registration records maintained by the DMV may be released under certain circumstances, which may vary depending on the method by which the request is made.⁴⁴ For example, the DMV *may not* release information contained in vehicle registration records in response to a *telephone inquiry*, unless requested by a peace officer acting in an official capacity or an official of the state, city, town, county, special district or other political subdivision, utilizing the obtained information for statutorily defined purposes.⁴⁵

On the other hand, the DMV *may* release information contained in vehicle registration records in response to a *written* request if the requestor completes and executes the proper DMV form. *Appendix C* provides a sample of the current form, which requires several pieces of information, including statements that show the requestor has the proper authority and that the information will be used for a lawful purpose.⁴⁶

The DMV reports that, during the 10-month period since its inception (Nov. 1, 2009, through Aug. 31, 2010), it received 18,719 requests for information contained in vehicle title and registration records and received \$37,810 in revenue for allowable fees and costs associated with these requests.⁴⁷

IV. Parks and Wildlife Department

The Texas Parks and Wildlife Department (TPWD) is responsible for regulating and issuing permits and licenses for recreational activities, such as hunting and fishing, game breeding and entry to and use of state park facilities.⁴⁸ As a result, TPWD collects personal information on individuals who purchase these recreational licenses, permits, products or services.

Except where authorized, the following information regarding a person who purchases products, licenses, or services may not be disclosed: name, address, telephone number, Social Security number, drivers license, and bank account/credit/charge card number.⁴⁹ [See *Appendix C* for a sample of the current order form] The information is also not releasable by TPWD when requested under the Public Information Act.⁵⁰ However, TPWD may disclose customer information to a federal or state law enforcement agency if the agency provides a lawfully issued subpoena.⁵¹ TPWD has adopted rules providing specific guidelines for the disclosure of that data.⁵²

⁴³ Tex. H.B. 3097, 81st Leg., R.S., (2009); *see also* Tex. Trans. Code Ann., § 1001

⁴⁴ Tex. Trans. Code Ann. §§ 502.008, 730.001

⁴⁵ Tex. Trans. Code Ann. § 502.008(a) (providing an exception when use is for tax purposes or for purposes of determining eligibility for a state public assistance program).

⁴⁶ *Id.*

⁴⁷ For purposes of this report, revenue from DMV (fiscal 2005-09) was submitted by TxDOT in its survey responses as the functions were still housed there during the relevant time periods being reviewed in this study.

⁴⁸ Tex. Parks & Wild. Code Ann., § 12.001

⁴⁹ *Id.* at (a)

⁵⁰ *Id.* at (b)

⁵¹ *Id.* at (e)

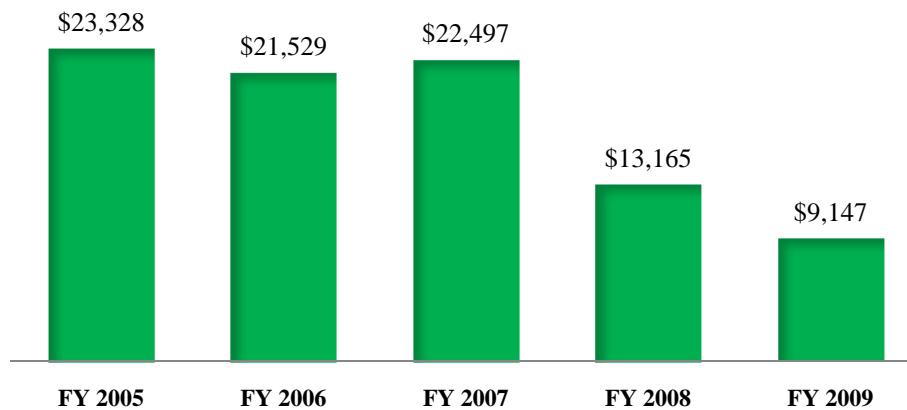
⁵² 31 Tex. Admin. Code Ann. §51.300 (Tex. Parks and Wildlife Dept.); adopted to be effective July 19, 2004, 29 *TexReg*6961.

TPWD is responsible for the following: registration, title and/or issuance of “certificates of numbers” for boats, boat motors, and personal watercraft;⁵³ and the licensing of party boat operators on inland waters,⁵⁴ marine dealerships, manufacturers and distributors.⁵⁵

Generally, all of these types of ownership records are public records.⁵⁶ However, the code bars TPWD from releasing the name or address of a person recorded in the vessel and outboard motor ownership records unless they receive a written request that states: (1) the requestor’s name and address; and (2) the use of the information is for a lawful purpose.⁵⁷ [See *Appendix C* for the current request form]

The amount of fees collected by TPWD for providing copies of records over the last five fiscal years is reflected in Exhibit 5-4.

Exhibit 5-4
TPWD Revenue from Release of Information (Fiscal 2005 - 2009)



⁵³ Tex. Parks & Wild. Code Ann. § 31.021; *See also*, Federal Boating Act of 1958 (shifting the responsibility of numbering vessels from the federal government to the states)

⁵⁴ *Id.* § 31.176

⁵⁵ *Id.* § 31.041

⁵⁶ *Id.* § 31.039(a)

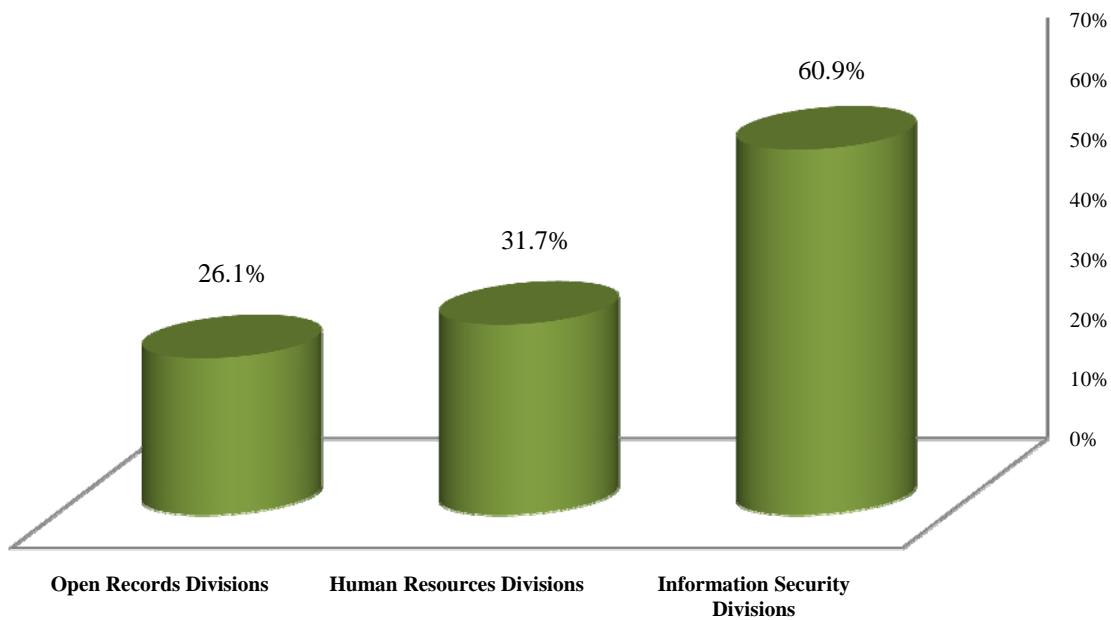
⁵⁷ *Id.* § 31.0391(a); *See also* Subsection (b) (providing that this Section does not apply to the release of information to a peace officer acting in an official capacity, or a state or public official who requests the information for tax purposes.)

Chapter VI: Agencies' and Institutions' Views on Security of Personally Identifiable Information, Training and Related Procedures

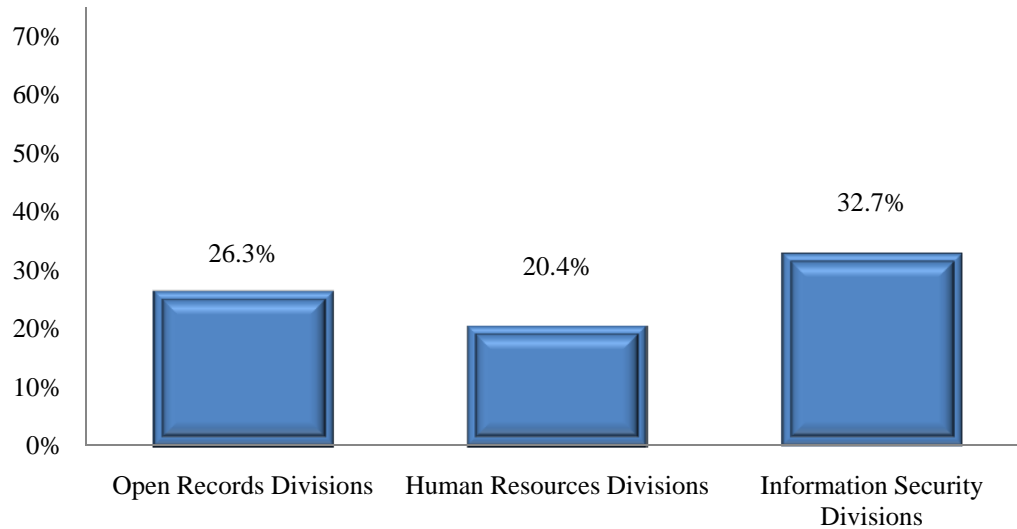
We asked the respondents about the safety and security of personally identifiable information. Along with specific security-related questions put to information security/technology (IS/IT) departments, questions were asked of other sections and divisions, such as human resources and open records, to shed light on the agency/institution's overall safety and security concerning personally identifiable information collection and storage.

Respondents were asked about a few proactive security measures used to help prevent the unintended disclosure of personally identifiable information. First, respondents were asked whether “security and/or privacy of personally identifiable information is discussed in weekly or monthly meetings?” Only 26 percent of open records divisions and approximately 32 percent of human resources divisions do (Exhibit 6-1). While the response rate from the IS/IT divisions was higher than the other two divisions, it was at a lower than expected level considering the magnitude of the issue, recent security breaches and overall concern for safety and security of personally identifiable information.

Exhibit 6-1
Security and/or Privacy of Personally Identifiable Information Discussed in Weekly or Monthly Meetings

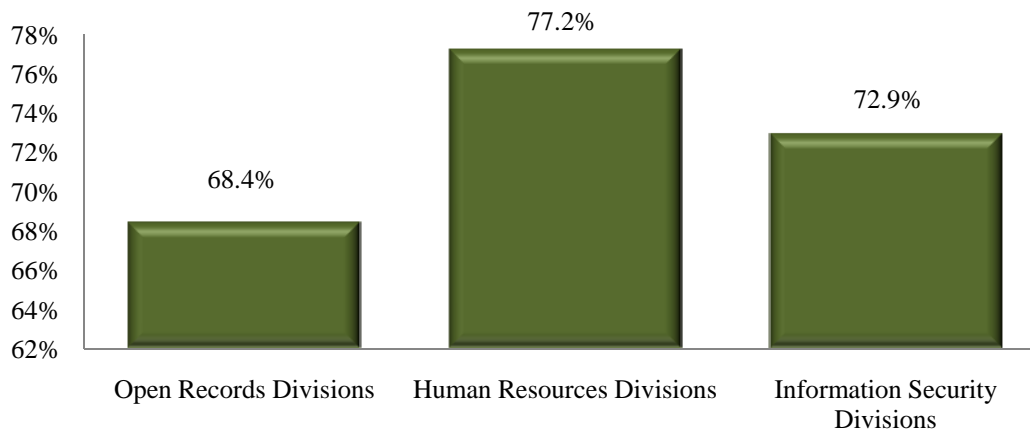


In response to whether or not “*there are postings or announcements in the work area reminding staff of the need for safety/security of personally identifiable information*,” our survey recorded significantly low positive responses from open records, human resources, and IT/IS divisions, ranging from 20 to 33 percent (Exhibit 6-2).

Exhibit 6-2**There are Postings or Announcements in the Work Area Reminding Staff of the Need for Safety/Security of Personally Identifiable Information**

Finally, respondents were asked whether, in their view, “*personnel receive adequate training in safety and assuring security of personally identifiable information.*” Affirmative responses were significantly higher than to the previous questions. Human resources respondents believed that their training was more adequate than IS/IT and open records divisions.

Exhibits 6-1 through 6-3 point to a need for consistent training and awareness for all sections/divisions in charge of collecting, managing and handling of personally identifiable information. Considering the magnitude of employees’ concern as well as recent security breaches, one expects to see affirmative response to those questions in the 90th or higher percentile.

Exhibit 6-3**Personnel Receive Adequate Training in Assuring Safety and Security of Personally Identifiable Information**

Our analysis showed that the likelihood of including personally identifiable information items in the periodic meetings was related to the size of the agencies. Exhibit 6-4 depicts the breakdown of responses based on the size of agencies. Agencies were grouped into small (50 or fewer employees), medium (51 to 99 employees) and large (100 or more employees) categories based on employees reported as of Jan. 1, 2010. Small agencies were less apt to discuss safety and security of personally identifiable information in their meetings and equally less likely to have postings and announcements addressing those issues. However, the perception about personnel receiving adequate training in assuring safety and security of personally identifiable information was comparable in all three groups. It is imperative to note that the numbers in Exhibit 6-4 reflect those responding to the IT/IS survey.

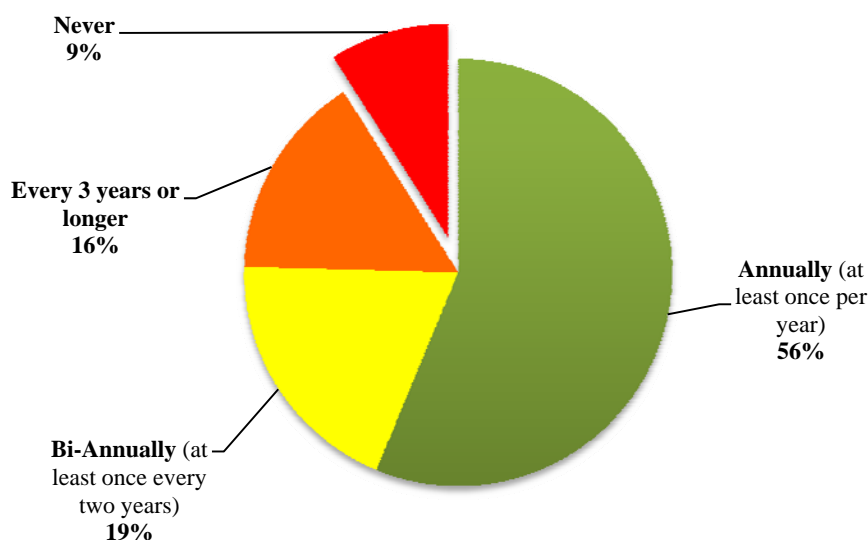
Exhibit 6-4
Concern for Safety and Security in Reference to Agency Size
IT/IS Survey

Agency/Institution	Yes		No	
	Number	Percent	Number	Percent
Security Discussed in Meetings				
Small	14	33.3%	28	66.7%
Medium	25	65.8%	13	34.2%
Large	14	93.3%	1	6.7%
Inst of Higher Ed	50	84.7%	9	15.3%
Security Postings or Announcements in the Work Area				
Small	5	11.4%	39	88.6%
Medium	12	32.4%	25	67.6%
Large	11	57.9%	8	42.1%
Inst of Higher Ed	27	45.0%	33	55.0%
Personnel Receive Adequate Training in Assuring Safety and Security of Personally Identifiable Information				
Small	31	83.8%	6	16.2%
Medium	31	86.1%	5	13.9%
Large	13	68.4%	6	31.6%
Inst of Higher Ed	49	79.0%	13	21.0%

Source: Data for this statistical table were extracted from the IT/IS survey instrument

The issue of whether IS/IT personnel receive adequate training was further assessed in a direct question in our IS Survey. Respondents were asked a closed-ended question regarding the “*frequency of IS/IT personnel receiving training in handling personally identifiable -related information.*” As Exhibit 6-5 reflects, the majority of respondents (56 percent) indicated that they receive training at least once per year, followed by those who were trained at least every two years (19 percent) and those who said training occurred once every three or more years (16 percent). The remaining 9 percent reported that their personnel have “never” received training in handling personally identifiable-related information (Exhibit 6-5).

Exhibit 6-5
Frequency of IT/IS Personnel Receiving Training in Handling Personally Identifiable Related Information



Standard Procedures and Security Safeguards:

Information security/technology divisions were asked whether “*safeguards were reviewed for effectiveness on regular basis.*” Of the 171 divisions surveyed, 86 percent responded yes and 14 percent said safeguards are not reviewed on a regular basis.

Those who responded affirmatively were asked about the frequency of those reviews. A significant majority of the respondents (81 percent) claimed reviews at least once per year. More than 15 percent conducted reviews every other year and 3.4 percent reviewed safeguards every three to four years.

Exhibit 6-6
Review of Information Security Safeguards

Question		Responses	
		Number	Percent
Are safeguards reviewed for effectiveness on a regular basis?			
	Yes	147	86.0%
	No	24	14.0%
If YES, how frequently?			
	More than once per year	43	29.3%
	Annually	76	51.7%
	Bi-Annually	23	15.6%
	Every 3-4 years	5	3.4%
	Every 5 or more years	0	0.0%

Chapter VII: Trends in Texas and Nationwide

Public Information in Texas

Texas, well-known for having a strong set of public information laws, operates one of the most transparent state governments in the country,⁵⁸ due in large part to several key provisions in the Public Information Act (the Act)⁵⁹ and Attorney General interpretations thereof. The Act operates under a presumption that unless there is a specific constitutional provision, statute or court order/decision creating an exception, the information possessed by a governmental body is considered public information.⁶⁰ The Act must also be liberally construed in favor of granting a request for information.⁶¹

Of course, there are specific exceptions to disclosure. For example, Subchapter C of the Act contains a laundry list of exceptions, including exceptions for student records, certain legal matters and photographs of peace officers.⁶² Recent legislation created some new statutory exceptions and modified others.

Recent Texas Legislation

In 2007, the 80th Legislature passed Senate Bill 123, which excepts certain information maintained by a municipality relating to the participation of minors in recreational activities.⁶³ Cities collect personal information of youths participating in city-sponsored recreational activities for purposes of emergency situations and to ensure the release of a child to the appropriate individual. Prior to the passage of this bill this information, including the child's name, age, home address, photograph, telephone number and names of parents or guardians was considered public information; it is now protected.⁶⁴

During the same session in 2007, the Legislature passed House Bill 1042, making changes to the "crime victim" exception. Under the old provision, the statute allowed crime victims to elect whether to allow public access to their personal information held by the crime victim's compensation division of the Attorney General's Office. With the passage of HB 1042, that information is now automatically confidential without the need of an election by the victim.⁶⁵

In 2009, the 81st Legislature added a new exception relating to the safety of public employees and officers of governmental bodies. Senate Bill 1068 added Section 552.151 to the Government Code, which excepts certain information relating to an employee or officer of a governmental body if, under the specific circumstances pertaining to the employee or officer, disclosure of the information would subject the person to a substantial threat of physical harm.⁶⁶

Attorney General Requests and Rulings

In addition to these legislative changes, there have been recent Attorney General requests and rulings relating to the release or protection of personally identifiable information.

⁵⁸ Better Government Association and Alper Services, *BGA - Alper Integrity Index* (2008) (a national study on states' transparency laws which ranked Texas No.7), available at www.bettergov.org/

⁵⁹ See Tex. Gov't Code Ann. § 552.001, et seq.

⁶⁰ See Op. Tex. Att'y Gen. No. H-436 (1974) and Tex. Att'y Gen. ORD-363 (1983), ORD-339 (1982), ORD-150 (1977), and ORD-91 (1975).

⁶¹ Tex. Gov't Code Ann. § 552.001(b)

⁶² See Tex. Gov't Code Ann. § 552.101, et seq. (for the full list of statutory exceptions listed in the Act)

⁶³ Tex. S.B. 123, 80th Leg., R.S., (2007)

⁶⁴ Tex. Gov't Code Ann. § 552.148

⁶⁵ Tex. H.B. 1042, 80th Leg., R.S., (2007)

⁶⁶ Tex. H.B. 1068, 81st Leg., R.S., (2009)

In December 2009, the Attorney General issued Open Record Decision 684, describing certain information that can be withheld without the necessity of seeking an Attorney General ruling.⁶⁷ Some of the types of information listed in this ruling include the following: direct deposit authorization forms; credit/debit/charge card numbers; fingerprints; and bank account numbers.

The Texas Ethics Commission recently asked the Attorney General whether documents containing personally identifiable information that are required to be attached to complaints filed with the Commission must be included when the Commission provides a copy of the complaint to the individual against whom the complaint was filed.⁶⁸ The Attorney General has yet to decide this matter.

Confidentiality of Personally Identifiable Information in the Courts

While the trend appears to be toward more protection of sensitive information, there are instances in which the Attorney General and the courts have ruled in favor of releasing information. For example, a 2008 opinion of the Third Court of Appeals indicates that neither common-law privacy⁶⁹ nor constitutional privacy protect the dates of birth of state employees; therefore, the information is public.⁷⁰ The case is currently pending before the Texas Supreme Court.

Clearly, Texas law recognizes the importance of operating an open and transparent government for the people it serves. Equally evident is the need to make adjustments to these laws as evolving technologies and circumstances make information more accessible. These same types of trends can be seen across the nation.

National Trends in Personally Identifiable Information and Open Records

Information gathered from pending legislation and statutes from other states indicates similar concerns to those facing Texas in trying to balance the growing public outcry for transparency in government with the ever-increasing need to protect individual privacy as identity theft escalates.

Trends in Transparency:

- Several states have taken steps to make public information more accessible to their citizens. For example, Arizona,⁷¹ Colorado,⁷² Connecticut,⁷³ Georgia⁷⁴ and South Dakota⁷⁵ have all proposed or enacted legislation to provide for posting public information online.

⁶⁷ Tex Att'y Gen. ORD-684 (2009)

⁶⁸ Letter from David A. Reisman, Executive Director, Texas Ethics Commission, to Honorable Greg Abbott, Attorney General of Texas (Aug. 10, 2010), *available at* www.oag.state.tx.us/opinions/opinions/50abbott/rq/2010/pdf/rq0910GA.pdf (hereinafter RQ-0910-GA).

⁶⁹ See Tex Att'y Gen. ORD-257 (1980) (citing *South v. Texas Industrial Accident Board*, 540 S.W. 2d 668 (Tex. 1976) for the proposition that "[i]n order to be excepted under the doctrine of common law privacy...information must contain highly intimate or embarrassing facts, the publication of which would be highly objectionable to a reasonable person, and, in addition, the information must be of no legitimate concern to the public.")

⁷⁰ *Id.*

⁷¹ HB 2115, (amending section 38-431.01, Arizona rev. statutes, relating to public meetings and proceedings), HB 2209, (amending sections 38-431.01, 38-431.02 and 41.1006, Arizona rev. statutes, relating to public notices of meetings), and HB 2282 (amending section 41.725, amending Title 41, Arizona rev. statutes, by adding Chapter 46, relating to revenues and expenditures of government monies), 49th Leg., 2nd Reg. Sess. (Ariz. 2010).

⁷² HB 10-1036, 67th Gen. Assem., 2nd Reg. Sess. (Colo. 2010) (Public School Financial Transparency Act).

⁷³ HB 5163, 2010 Gen. Assem., Feb. Sess. (Conn. 2010) (establishment of a searchable database for state expenditures).

⁷⁴ HB 122, 2010 Gen. Assem., Reg. Sess. (Ga. 2010) (requiring each local government having an annual budget in excess of \$1 million to post certain information to a website accessible by the public)

- Pennsylvania's "Right to Know Act" is a series of laws designed to guarantee that the public has access to public records of governmental bodies.⁷⁶ Pennsylvania is also considering legislation to post all public employee salaries online (SB 107)⁷⁷

Trends in Privacy Protection

- Appendix F shows that about half of the states protect the information in state employee personnel files, including their date of birth. Several states – including Arizona, Illinois, Kansas, New Jersey, North Dakota and Nebraska – exempt from public disclosure state employee personnel files with exceptions for such things as employment history, pay grade, gross salary, classification and employing agency.
- Arizona has enacted legislation specifying which types of disciplinary information relating to health professionals may be posted on regulatory board websites.⁷⁸
- Proposed California legislation would prohibit a person from knowingly disclosing or using regulated records that include prescription information containing individual identifying information for marketing a prescribed product.⁷⁹
- In Illinois, less than a year after approving several significant changes to the state's Freedom of Information Act laws to make public records more accessible, legislators have introduced a series of bills attempting to make access more difficult.⁸⁰ House Bill 5154 would bar disclosure of performance evaluations of state and local law enforcement personnel.⁸¹ Senate Bill 2978 would allow agencies to withhold records in employee disciplinary cases absent criminal convictions.⁸²
- Legislation is under consideration in Florida to exempt from public records requirements certain voter registration information and specified personal identifying information of stalking victims.⁸³
- Maine has enacted legislation to restrict access to birth certificates and marriage records to only the individual(s) on the record or their "spouse, registered domestic partner, descendants, parents or guardians or that person's duly designated attorney."⁸⁴
- Georgia legislation prohibits certain crime scene photos from release. Alabama has enacted legislation exempting 9-1-1 recordings from being released to the public under the state's public-records laws and requiring a court order to compel their disclosure.⁸⁵

State Entities Overseeing Individual Privacy Rights:

California has created an agency dedicated to promoting and protecting the privacy rights of consumers.⁸⁶ Hawaii has the Information and Privacy Security Council, comprised of 12 members from various state government entities "to protect the security of personal information collected and maintained by state and county government agencies."⁸⁷

⁷⁵ "Open SD", available at <http://open.sd.gov/> (website for easy public access to South Dakota government information).

⁷⁶ Act 3 of 2008 (Eff: 01/01/09) (Amended in 2009 to state that all documents will be presumed to be open to the public unless the [state] agency holding them can prove otherwise).

⁷⁷ S.B. 107, General Assembly, Reg. Session, (Pa. 2009-2010).

⁷⁸ H.B. 2545, 49th Leg., 2nd Reg. Sess. (Ariz. 2010) (Relating to Professions and Occupations).

⁷⁹ A.B. 2112, 2009-10 Gen. Assem., Reg. Sess. (Cal. 2010)

⁸⁰ Bruce Rushton, "FOIA overhaul already under siege by legislators" *State Journal-Register* (Feb. 15, 2010), <http://www.sj-r.com/top-stories/x2077694644/Legislators-move-to-roll-back-Freedom-of-Information-Act-changes>

⁸¹ H.B. 5154, 2010 Gen. Assem., Reg. Sess. (Ill. - Approved by governor, July 2010)

⁸² S.B. 2978, 96th Gen. Assem., Reg. Sess., (Ill. 2009-2010).

⁸³ S.B. 2188, 2010 Leg., Reg. Sess. (Fla. 2010).

⁸⁴ H.P. 1271, 124th Leg., 2nd Reg. Sess. (Me. 2010)

⁸⁵ H.B. 159, 2010 Leg., Reg. Sess. (Ala. 2010)

⁸⁶ S.B. 129, 1999-00 Gen. Assem., Reg. Sess. (Cal. 2000) (California Office of Privacy Protection, opened in 2001)

⁸⁷ S.B. 2803, SC1, HD1, CD1, 24th Leg., Reg. Sess., (Ha. 2008) (Hawaii Information Privacy & Security Council).

Federal Legislation:

At the federal level, the E-Government Act of 2002 (Public Law 107-347) requires federal agencies to conduct “privacy impact assessments when there are new collections of, or new technologies applied to, [personally identifiable information].”⁸⁸ The Homeland Security Act of 2002 as amended⁸⁹ created the chief privacy officer at the Department of Homeland Security (DHS), whose responsibilities include ensuring that privacy *and* transparency initiatives are implemented throughout the department.⁹⁰

According to the DHS website, the privacy office was established to preserve and enhance privacy protections for all individuals, to promote transparency of department operations and to serve as a leader in the federal privacy community.⁹¹ The office works to ensure that privacy considerations are addressed when planning or updating DHS programs, systems and initiatives and ensures that technologies used do not erode privacy protections.⁹²

Legislation is also being proposed to require security policies and procedures to protect data containing personally identifiable information, and to provide nationwide notice in the event of a security breach.⁹³ Other bills strive to prevent and mitigate identity theft, ensure privacy, provide notice of security breaches and enhance criminal penalties, law enforcement assistance and other protections against security breaches, fraudulent access and misuse of personally identifiable information.⁹⁴

⁸⁸ Department of Homeland Security, *Authorities and Responsibilities of the Chief Privacy Officer*, available at www.dhs.gov/xabout/structure/gc_1265225837602.shtm

⁸⁹ Codified at 6 U.S.C. 552 (2002)

⁹⁰ www.dhs.gov/xabout/structure/gc_1265225837602.shtm (emphasis added)

⁹¹ Department of Homeland Security, *About the Privacy Office*, www.dhs.gov/xabout/structure/editorial_0510.shtm

⁹² *Id.*

⁹³ See S. 3742, 111th Cong., 2nd Sess. (2010) (Data Security and Breach Notification Act of 2010)

⁹⁴ See S. 1490, 111th Cong., 1st Sess. (2009) (Personal Data Privacy and Security Act of 2009)

Chapter VIII: Conclusion & Recommendations

Conclusion

On Aug. 7, 2009, State Sen. Robert Duncan, Chair of the Senate Committee on State Affairs with jurisdiction over the Public Information Act, asked the Comptroller's office "to study and analyze and prepare a report on the amount and types of personally identifiable information collected by each state governmental body." The project included a request for exploration of the volume and types of personally identifiable information collected and maintained by all state agencies and institutions of higher education, along with an analysis of the disclosure and sale of personally identifiable information under Chapters 521, 522, and 730 of the Texas Transportation Code by the state agencies to which those chapters apply.

Data for this report were collected through development of six surveys and collection of information from various programs and divisions within each state agency and institution of higher education. Three strategies were employed to improve the validity of the surveys including an assessment by a team of experts and a pilot survey among a selected number of agencies and institutions.

In May 2010, the surveys were e-mailed to all participating agencies/institutions along with a copy of Sen. Duncan's letter, instructions and guidelines. The agencies were given two weeks to complete and return the surveys. More than 2,000 were completed and returned.

Our research revealed that state agencies and public universities have experienced significant information security-related incidents in the last five years. In 2009 alone, nine Texas metro areas made the Federal Trade Commission's top 50 list of largest metropolitan areas with the most identity theft consumer complaints. Many of those incidents involved identity theft relating to government documents or benefits. Those incidents have resulted in the disclosure of personally identifiable information such as Social Security numbers and dates of birth and have diminished the level of trust between the governmental body or university and the people served.

The data analysis revealed that as of Jan. 1, 2010, the participating state agencies and institutions of higher education collected and stored over 5 billion pieces of personally identifiable information – 4,358,936,859 (86.9 percent) residing with state agencies and 657,339,341 (13.1 percent) maintained by institutions of higher education.

First and last names (324 million) were the items of personally identifiable information most frequently collected and maintained by state agencies followed by home address (309 million), dates of birth (297 million) and Social Security numbers (more than 229 million). Other high-ranking personally identifiable information items were personal cell/home telephone numbers (202 million), medical information (214 million), personal e-mail addresses (155 million) and drivers license numbers (more than 152 million).

The same trend was noted in personally identifiable information items collected by institutions of higher education: First and last names were the most frequent personally identifiable information items collected (more than 36 million), followed by dates of birth (nearly 32 million), personal cell/home telephone number (more than 31 million) and home address (more than 31 million).

State agencies and institutions of higher education received 1,070,991 open records requests in fiscal 2009. Of those, more than 99 percent were received by state agencies and less than 1 percent by

institutions of higher education. Of those, 712,293 (66 percent) asked for personally identifiable information.

In fiscal 2009 less than one percent of personally identifiable information-related requests were referred to the Office of the Attorney General (OAG). Of those, the majority were ruled to be protected (1,118 out of 1,247 requests –nearly 90 percent).

Nearly three-quarters of respondents (143 agencies/institutions) indicated that they receive revenue for sharing information. Only 22.9 percent (44 agencies/institutions) said that they do not receive revenue for sharing information. On average, all agencies and institutions received approximately \$64.5 million per year, of which more than 99 percent was received by state agencies with less than 1 percent from the institutions of higher education. The Texas Department of Public Safety led all state agencies in generating revenue through sharing information in fiscal 2009, followed by the Secretary of State's office and the Railroad Commission.

Only 26 percent of open records divisions and close to 32 percent of human resources divisions discuss safety and security of personally identifiable information in their weekly or monthly meetings, and less than one-third of IS/IT, human resources and open records divisions are adequately trained in collection, management and handling of personally identifiable information.

Finally, in response to whether a review of safeguards was conducted for effectiveness on a regular basis by IS/IT divisions, 86 percent responded positively with 24 agencies (14 percent) indicating that safeguards are not reviewed on a regular basis. Of those who reviewed the safeguards on a regular basis, a significant majority mentioned that it was done once or more per year (86 percent). More than 15 percent said it was done every other year and 3.4 percent indicated it was conducted every three to four years.

Recommendations

The following recommendations are designed to help protect employees of governmental bodies and private individuals who share information with these bodies. These recommendations are based on survey responses, identity theft statistics and nationwide trends regarding the protection of personal information and transparency.

1. The Legislature should consider creating an information security council or review board, consisting of representatives from small, medium and large sized agencies and institutions of higher education. For example, some entities could include the following: Health and Human Services Commission, Department of Public Safety, Department of Information Resources, the Information Technology Council for Higher Education and the Comptroller of Public Accounts. The Office of the Attorney General and the State Library and Archives Commission could also serve as ex officio, non-voting members of the council.
2. The information security council or review board referenced above should at minimum have the authority over, and be responsible for:
 - a) Appointing an advisory committee or committees to assist the council.
 - b) Creating model security awareness training policies and procedures for state governmental bodies, particularly those collecting, handling, transferring, sharing and/or releasing personally identifiable information, and should at minimum address:

- i. Destruction, deletion, and/or purging of unwanted personally identifiable information in coordination with the State Library and Archives Commission and the Records Management Interagency Coordinating Council;
 - ii. Procedures agencies can use to help ensure confidentiality policies remain consistent as data is transferred to other agencies or entities;
 - iii. Increasing security awareness levels across all state agencies and institutions;
 - iv. Developing techniques and recommendations for agencies and institutions to effectively communicate their personally identifiable information confidentiality policies and procedures to third-party vendors who may access personally identifiable information residing in state databases;
 - v. Adopting uniform guidelines relating to the security of laptops, removable data storage devices, and communication devices, including, but not limited to personal digital assistants, cell phones and smart phones.
 - vi. Regular assessments of the types of personally identifiable information collected and maintained by agencies and institutions to determine if such information is necessary.
- c) Making recommendations in a report to the Legislature regarding:
- i. An update on statewide privacy issues, including the increased or decreased threat of identity theft, the status of the model personally identifiable information training policies and the overall protection of personally identifiable information;
 - ii. Whether the information public employees may elect to protect under Section 552.024, Gov't Code (Social Security number, home address, home phone and family member information), should be automatically protected without the need for an election (according to Comptroller data, more than 97 percent of employees at state agencies and 86 percent of employees at institutions of higher education have elected not to share at least one of the above pieces of information);
 - iii. Whether agencies and institutions should be required to monitor and/or conduct regular inventories or audits of the number and types of personally identifiable information they collect to determine if any items may no longer be necessary for the effective functioning of the agency or institution; and
 - iv. Whether, in light of an increased threat of fraud, identity theft or new technologies and circumstances that may impact privacy considerations, the Legislature should consider adding protections that would allow governmental bodies to redact or withhold from public release drivers license numbers, Social Security numbers (or variations thereof, including taxpayer identification number, vendor identification number, and Texas identification number), home addresses, home telephone numbers, family member information and dates of birth.

While personally identifiable information such as date of birth or Social Security number might not have been considered “highly intimate” information in 1980, most individuals today would consider it to be sensitive in nature, particularly in conjunction with their complete name, work information, sex, race and ethnicity. In addition, it is clear that this type of data is highly sought out by identity thieves as they attempt to profit from its theft and subsequent use. Half of the

states currently provide some sort of protection for dates of birth and other pieces of sensitive information and more appear to be trending in that direction. Several states, including Arizona, Illinois, Kansas, New Jersey, North Dakota and Nebraska, exempt state employee personnel files with exceptions for name, gross salary and employing agency. Several participating agencies indicated there is a need to protect this type of information from disclosure under the Public Information Act.

A regular review of privacy issues will help keep the state abreast of the ever-changing trends in this arena and assure the public that the state takes the protection of its personally identifiable information seriously. Such reviews will also assure the public that the data being collected by governmental bodies is, in fact, necessary for the successful management and operation of each agency, division or program.

- d) Making recommendations to agencies and institutions of higher education on changes to state forms, so the public is more aware of which types of personally identifiable information being provided are public under the Public Information Act.

Agencies are already required to provide statements under the Federal Privacy Act explaining why Social Security numbers are being collected and what use will be made of them and advising of an individual's right to correct false information or to see information about oneself under Government Code Chapter 559. This recommendation should help add transparency to many state processes and create more public awareness of which types of information are protected and which are not.

- e) Ensuring one public information/privacy website exists and is accessible to the public.
 - i. The website should provide, at a minimum, the following: a complete list of public information officers and/or privacy officers at state agencies and institutions and their contact information; links to all state agencies and their cost and access policies; and a consistent and convenient e-mail address to submit requests and obtain needed transparency resources.
 - ii. Agencies should also designate a person to address individual concerns or special circumstances under which an individual's personally identifiable information should not be publicly disclosed at least until a determination can be made by the Attorney General.

Currently, there is no complete contact list for public information officers or privacy officers at state agencies. Creating a comprehensive list at the state level could be useful for members of the public who have concerns about personally identifiable information.

- f) Ensuring that state agencies and institutions of higher education use consistent definitions to help determine which data types are sensitive, confidential or public. And, in coordination with the Public Electronic Services On-the-Internet (PESO) workgroup, help ensure that agencies create, where administratively and economically feasible, an easily accessible website or portal for the types of data that are determined to be public and not sensitive in nature, so the public can easily view and retrieve the data without having to make an official open record request. This may help reduce the number of open record requests, thereby helping to reduce instances that may result in the unnecessary or improper inclusion of sensitive or confidential data.
- g) Generally, the council should be subject to the Texas Open Meetings Act (OMA), with meetings open to the public for comment. However, the council should not be required to openly deliberate on the following: (1) security assessments or deployments relating to information resources technology; (2) network security information as described by Section 2059.055(b), Gov't Code; or (3) the deployment, or specific occasions for implementation, of security personnel, critical

infrastructure, or security devices. The council must ensure that the appropriate workgroups, committees and experts in the areas of privacy, public information, security of electronic information and other needed areas of expertise are invited to assist and provide needed technical assistance.

Appendix A:

Request Letter from Sen. Robert Duncan



ROBERT DUNCAN
STATE SENATOR
DISTRICT 28

RECEIVED

AUG 10 2009

EXEC. ADMIN.
CORRESPONDENCE

COMMITTEES:
STATE AFFAIRS, CHAIR
FINANCE
HIGHER EDUCATION
JURISPRUDENCE
NATURAL RESOURCES

August 7, 2009

The Honorable Susan Combs
Post Office Box 13528, Capitol Station
Austin, TX 78711-3528

Dear Comptroller Combs,

During the 80th Legislature, 19 bills were filed regarding the protection of personal information and open records. The Public Information Act was originally enacted in 1973, long before the age of technology and instant access to any information at any time of the day. Personally identifiable information, name, address, date of birth, driver's license and social security numbers that we once provide upon request has become the foundation for identity theft. As the Internet becomes more and more commonplace, identity theft has become a problem of pandemic proportions.

State government possesses a tremendous amount of information not only on the state's employees but also from every business or person who comes in contact with the state. We need to study the data state government has in its possession, the data it requires from persons in contact with state government and the safeguards of that data.

As the state's Comptroller of Public Accounts, you are in a unique position to study and report on data that is collected and held by the state government. I am requesting that you study the following and prepare a detailed report on your findings.

Report Content

The comptroller shall study and analyze and prepare a report on the amount and types of personally identifiable information collected by each state governmental body. The analysis must include a study of the disclosure and sale of personally identifiable information under Chapters 521, 522, and 730, Transportation Code, by the state agencies to which those chapters apply.

LUBBOCK DISTRICT OFFICE:
1500 BROADWAY
SUITE 902
LUBBOCK, TEXAS 79401
(806) 762-1122
1-800-546-9928
FAX (806) 749-2828
DIAL 711 FOR RELAY CALLS

CHILDRESS DISTRICT OFFICE:
119 AVENUE B NW
CHILDRESS, TEXAS 79201
(940) 937-0909
(888) 887-7027
FAX (940) 937-6994
DIAL 711 FOR RELAY CALLS

CAPITOL OFFICE:
ROOM 3E.10
P.O. Box 12068
AUSTIN, TEXAS 78711
(512) 463-0128
(800) 322-9538
FAX (512) 463-2424
DIAL 711 FOR RELAY CALLS

SAN ANGELO DISTRICT OFFICE:
36 WEST BEAUREGARD
SUITE 510
SAN ANGELO, TEXAS 76903
(915) 481-0028
1-800-558-9928
FAX (915) 655-2541
DIAL 711 FOR RELAY CALLS

The report requested by this study shall

(a) identify the personally identifiable information collected by each state governmental body and

(b) the report must contain the comptroller's recommendations for legislation regarding personally identifiable information collected by a state governmental body, including recommendations on:

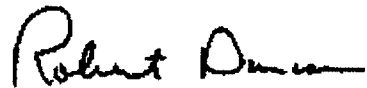
(1) whether each state governmental body should continue to collect or maintain personally identifiable information; and

(2) whether to amend the public information law to further limit the types of personally identifiable information that may be withheld from disclosure; and

(3) the effect of the recommendations made under this section.

Finally, I request this report be prepared and delivered to my office by December 1, 2010.

Yours very truly,

A handwritten signature in black ink, appearing to read "Robert Duncan". The signature is fluid and cursive, with the first name "Robert" being more prominent than the last name "Duncan".

Robert Duncan

Appendix B:

Types of Personally Identifiable Information Held by State Agencies and Public Institutions of Higher Education

- Exhibit 3-4, Total Pieces Personally Identifiable Information Collected by Agencies and Institutions of Higher Education Sorted by Grouping (Member, Client, Student, Employee, Applicants, Contractor)
- Exhibit B-1, Totals by State Agency and Institution of Higher Education
- Exhibit B-2, Annual Number and Percentage of Pieces of Personally Identifiable Information belonging to Employment Applicants
- Exhibit B-3, Number and Percent of Students', Clients', and Service Recipients' Information by State Agency and Institution of Higher Education
- Exhibit B-4, Number and Percent of Contractors' and Bidders' Information by State Agency and Institution of Higher Education

Exhibit 3-4
Number of Personally Identifiable Information
Collected and Stored by State Agencies and Institutions of Higher Education in Texas
as of January 1, 2010

Personally Identifiable Information	Information Collected From						Total
	Members	Clients/ Service Recipients/ Others	Students	Employees/ Former Employees	Employment Applicants	Contractors/Bidders/ Consultants	
First and last name	5,050,911	311,034,572	35,608,396	1,882,650	2,633,988	4,177,447	360,387,964
Home address	4,895,050	308,563,396	20,119,339	1,882,650	2,446,116	2,350,491	340,257,042
Date of birth	4,944,197	284,580,531	33,260,964	1,882,594	1,827,372	2,154,252	328,649,910
Social Security number	4,871,486	213,730,524	32,351,704	1,882,650	1,886,448	3,926,264	258,649,076
Personal cell/home phone number	4,858,019	201,596,123	20,357,333	1,874,351	2,452,464	2,578,214	233,716,504
Medical information	3,318,890	214,326,085	10,071,014	1,548,128	1,277,772		230,541,889
Personal email address	4,089,074	152,871,383	21,281,744	1,356,017	2,610,588	3,014,651	185,223,457
Driver's license number	2,372,321	149,139,897	7,841,682	1,610,906	1,912,908	2,440,715	165,318,429
Death certificates	2,958,054	135,618,483	4,796,351				143,372,888
Birth certificates	2,860,902	129,996,371	5,833,549	1,113,006	169,620	9,611	139,983,059
Info about employee's spouse	3,472,206	112,476,442	11,755,070	1,472,257		5,028	129,181,003
Birth place	2,604,283	112,560,541	9,857,695	615,199	246,300	1,676,634	127,560,652
Info about employee's child(ren)	3,012,178	110,047,332	11,448,232	1,705,315		5,031	126,218,088
Employment date	3,699,051	105,202,048	9,402,414	1,882,650	2,433,756	706,666	123,326,585
Physically impaired information	2,069,325	100,914,051	16,588,131	1,422,560	1,295,832	80,000	122,369,899
Account no login information	1,900,322	106,993,079	10,198,871	671,601		14,709	119,778,582
Texas taxpayer ID	1,801,727	103,281,169	6,347,095	25,783		3,596,190	115,051,964
Educational background	2,115,306	82,166,144	21,538,580	1,852,181	2,487,732	1,636,445	111,796,388
Mother's maiden name	2,471,107	93,626,458	2,701,878	94,333	105,684	1,676,552	100,676,012
Banking information	3,099,694	87,951,824	4,475,944	1,599,102		2,375,090	99,501,654
Divorce decrees	2,898,028	89,016,448	5,199,614				97,114,090
Emergency contact information	83,848	78,064,388	14,706,907	1,844,232		304,137	95,003,512
Immigration/naturalization	1,804,364	68,101,294	20,118,771	1,859,567	413,244	1,894,467	94,191,707
Credit card/debit card number	884,659	80,014,761	6,594,809	156,739		1,586,941	89,237,909
Motor vehicle information	1,303,350	79,175,488	3,644,628	1,032,083		10,028	85,165,577
Substance abuse related information	919,000	74,602,440	3,542,815	1,135,090	1,227,792	3,000	81,430,137
Federal employment ID nc	6,540	65,471,173	3,985,706			3,522,165	72,985,584
Criminal record	924,590	58,995,257	4,659,670	1,691,431	1,758,336	900,573	68,929,857
Federal income tax information	2,665,493	45,324,234	9,021,025			2,402,331	59,413,083
Name of employees	737,986	47,325,714	6,282,137			1,697,389	56,043,226
Passport number	2,106,195	40,267,300	9,314,005	1,481,546		1,663,929	54,832,975
Photo	1,846,281	42,157,576	6,558,408	1,310,132	191,868	2,340,602	54,404,867
Loan information		46,728,243	5,990,435	460,588		155,778	53,335,044
Customer list	6,467	47,467,584	3,336,998			1,985,930	52,796,979
Business/personal finan statements	73,628	39,201,702	4,312,831	437,862		3,288,093	47,314,116
Handwriting sample	1,419,976	33,158,596	2,971,147	231,398	209,388	2,287,945	40,278,450
Lien information	2,353,350	35,509,660	439,944			199,530	38,502,484
Fingerprints	17,000	35,673,655	1,073,708	720,968	78,360	548,502	38,112,193
Accounting records	79,113	23,637,657	4,649,243			689,451	29,055,464
Wills	1,360,026	21,751,650	2,213,584				25,325,260
Credit history		20,954,435	2,100,947	44,380		206,443	23,306,205
Name/info of previous bus. owner	60,026	17,761,429	876,281			1,738,816	20,436,552
Bond information		9,373,556	1,003,693			2,563,167	12,940,416
Tax violations	1,300,000	5,378,409	1,653,575	64,401		2,435,420	10,831,805
Tax preparer information	60,026	7,339,175	2,293,994			42,520	9,735,715
Retina or iris image		4,483,034	94,000				4,577,034
Qualification information						3,543,417	3,543,417
Business insurance information						3,445,465	3,445,465
Bid/contract/consultation amount						3,201,089	3,201,089
Contracts						3,012,058	3,012,058
Business capacity information						2,979,959	2,979,959
Contract/bid/consultation history						2,971,555	2,971,555
Reference check						2,920,355	2,920,355
Work phone number					2,410,704		2,410,704
Background/reference information					2,103,480		2,103,480
Outside employment				1,254,690			1,254,690
Prior performance evaluations				1,197,085			1,197,085
Other	1,332,762	93,614,059	14,327,711	315,470	432,564	412,491	110,435,057
Total	90,706,811	4,327,225,370	436,802,572	41,611,595	32,612,316	87,377,536	5,016,336,200

Exhibit B-1
Number and Percentage of Personally Identifiable Information Items
by State Agencies and Institutions of Higher Education
as of January 1, 2010

Personally Identifiable information	State Agencies		Institutions of Higher Education		Total
	Number	Percent	Number	Percent	
First and last name	324,013,200	89.91%	36,374,764	10.09%	360,387,964
Home address	308,944,996	90.80%	31,312,046	9.20%	340,257,042
Date of birth	296,772,680	90.30%	31,877,230	9.70%	328,649,910
Social Security number	229,217,021	88.62%	29,432,055	11.38%	258,649,076
Personal cell/home phone number	202,381,047	86.59%	31,335,457	13.41%	233,716,504
Medical information	214,058,519	92.85%	16,483,370	7.15%	230,541,889
Personal email address	154,962,603	83.66%	30,260,854	16.34%	185,223,457
Driver's license number	152,259,981	92.10%	13,058,448	7.90%	165,318,429
Death certificates	136,582,235	95.26%	6,790,653	4.74%	143,372,888
Birth certificates	133,361,644	95.27%	6,621,415	4.73%	139,983,059
Info about employee's spouse	112,121,307	86.79%	17,059,696	13.21%	129,181,003
Birth place	114,029,118	89.39%	13,531,534	10.61%	127,560,652
Info about employee's child(ren)	110,738,910	87.74%	15,479,178	12.26%	126,218,088
Employment date	109,496,225	88.79%	13,830,360	11.21%	123,326,585
Physically impaired information	111,935,001	91.47%	10,434,898	8.53%	122,369,899
Account number login information	106,693,098	89.08%	13,085,484	10.92%	119,778,582
Texas taxpayer ID	106,106,110	92.22%	8,945,854	7.78%	115,051,964
Educational background	93,806,800	83.91%	17,989,588	16.09%	111,796,388
Mother's maiden name	95,660,072	95.02%	5,015,940	4.98%	100,676,012
Banking information	91,004,722	91.46%	8,496,932	8.54%	99,501,654
Divorce decrees	91,924,826	94.66%	5,189,264	5.34%	97,114,090
Emergency contact information	75,273,317	79.23%	19,730,195	20.77%	95,003,512
Immigration/naturalization	78,969,436	83.84%	15,222,271	16.16%	94,191,707
Credit card/debit card number	79,687,070	89.30%	9,550,839	10.70%	89,237,909
Motor vehicle information	81,160,278	95.30%	4,005,299	4.70%	85,165,577
Substance abuse related information	71,830,280	88.21%	9,599,857	11.79%	81,430,137
Federal employment ID number	66,557,540	91.19%	6,428,044	8.81%	72,985,584
Criminal record	62,498,124	90.67%	6,431,733	9.33%	68,929,857
Federal income tax information	48,820,421	82.17%	10,592,662	17.83%	59,413,083
Name of employees	46,999,420	83.86%	9,043,806	16.14%	56,043,226
Passport number	43,086,921	78.58%	11,746,054	21.42%	54,832,975
Photo	39,850,033	73.25%	14,554,834	26.75%	54,404,867
Loan information	46,917,582	87.97%	6,417,462	12.03%	53,335,044
Customer list	47,323,892	89.63%	5,473,087	10.37%	52,796,979
Business or personal financial statements	39,394,968	83.26%	7,919,148	16.74%	47,314,116
Handwriting sample	35,740,966	88.73%	4,537,484	11.27%	40,278,450
Lien information	37,524,893	97.46%	977,591	2.54%	38,502,484
Fingerprints	36,518,482	95.82%	1,593,711	4.18%	38,112,193
Accounting records	24,291,730	83.60%	4,763,734	16.40%	29,055,464
Wills	22,731,650	89.76%	2,593,610	10.24%	25,325,260
Credit history	21,160,264	90.79%	2,145,941	9.21%	23,306,205
Name and or info of previous business owner	17,575,845	86.00%	2,860,707	14.00%	20,436,552
Bond information	9,682,462	74.82%	3,257,954	25.18%	12,940,416
Tax violations	7,434,928	68.64%	3,396,877	31.36%	10,831,805
Tax preparer Information	7,392,486	75.93%	2,343,229	24.07%	9,735,715
Retina or iris image	4,483,034	97.95%	94,000	2.05%	4,577,034
Qualification information	1,002,948	28.30%	2,540,469	71.70%	3,543,417
Business insurance information	907,372	26.34%	2,538,093	73.66%	3,445,465
Bid/contract/consultation amount	928,173	29.00%	2,272,916	71.00%	3,201,089
Contracts	840,581	27.91%	2,171,477	72.09%	3,012,058
Capacity information	886,150	29.74%	2,093,809	70.26%	2,979,959
Contract/bid/consultation history	788,731	26.54%	2,182,824	73.46%	2,971,555
Reference check	418,215	14.32%	2,502,140	85.68%	2,920,355
Work phone number	1,507,056	62.52%	903,648	37.48%	2,410,704
Background/reference information	1,644,984	78.20%	458,496	21.80%	2,103,480
Outside employment	459,400	36.61%	795,290	63.39%	1,254,690
Prior performance evaluations	577,112	48.21%	619,973	51.79%	1,197,085
Other	100,501,151	91.00%	9,933,906	9.00%	110,435,057
Total	4,459,438,010	88.90%	556,898,190	11.10%	5,016,336,200

Exhibit B-2

Number and Percentage of Employment Applicants Personally Identifiable Information by State Agencies and Institutions of Higher Education, per Year

Personally Identifiable information	State Agencies		Institutions of Higher Education		Total
	Number	Percent	Number	Percent	
Name	1,699,992	64.54%	933,996	35.46%	2,633,988
Personal e-mail address	1,678,704	64.30%	931,884	35.70%	2,610,588
Educational background	1,560,360	62.72%	927,372	37.28%	2,487,732
Personal cell home phone number	1,518,480	61.92%	933,984	38.08%	2,452,464
Home address	1,512,120	61.82%	933,996	38.18%	2,446,116
Employment data	1,503,360	61.77%	930,396	38.23%	2,433,756
Work phone number	1,507,056	62.52%	903,648	37.48%	2,410,704
Background/reference check	1,644,984	78.20%	458,496	21.80%	2,103,480
Driver's license number	1,490,556	77.92%	422,352	22.08%	1,912,908
Social security number	1,442,964	76.49%	443,484	23.51%	1,886,448
Date of birth	1,364,976	74.70%	462,396	25.30%	1,827,372
Criminal record	1,212,252	68.94%	546,084	31.06%	1,758,336
Physically impaired information	1,187,400	91.63%	108,432	8.37%	1,295,832
Medical information	1,222,812	95.70%	54,960	4.30%	1,277,772
Substance abuse related information	1,173,552	95.58%	54,240	4.42%	1,227,792
Immigration naturalization	132,036	31.95%	281,208	68.05%	413,244
Birth place	91,260	37.05%	155,040	62.95%	246,300
Handwriting Sample	207,948	99.31%	1,440	0.69%	209,388
Photo	83,916	43.74%	107,952	56.26%	191,868
Birth certificate	88,932	52.43%	80,688	47.57%	169,620
Mother's maiden name	300	0.28%	105,384	99.72%	105,684
Finger prints	78,120	99.69%	240	0.31%	78,360
Other	302,760	69.99%	129,804	30.01%	432,564
Total	22,704,840	69.62%	9,907,476	30.38%	32,612,316

Exhibit B-3

Number and Percentage of Students, Clients, and Service Recipients Personally Identifiable Information by State Agencies and Institutions of Higher Education

as of January 1, 2010

Personally Identifiable Information	State Agencies		Institutions of Higher Education		Total
	Number	Percent	Number	Percent	
Name	319,814,766	91.64%	29,190,130	8.36%	349,004,896
Home address	305,949,945	92.46%	24,948,624	7.54%	330,898,569
Date of birth	293,945,877	91.82%	26,192,698	8.18%	320,138,575
Social Security	225,385,144	90.77%	22,911,180	9.23%	248,296,324
Medical information	211,966,288	94.11%	13,260,477	5.89%	225,226,765
Personal cell Home phone Number	199,380,334	88.93%	24,821,425	11.07%	224,201,759
Personal email address	151,519,893	86.22%	24,206,959	13.78%	175,726,852
Driving Records	149,320,016	95.18%	7,558,633	4.82%	156,878,649
Death Certificates	136,582,235	96.21%	5,377,626	3.79%	141,959,861
Birth Certificates	132,787,769	96.72%	4,503,053	3.28%	137,290,822
Info about employees spouse	111,473,104	89.00%	13,774,390	11.00%	125,247,494
Birth place	113,599,282	91.64%	10,367,013	8.36%	123,966,295
Info about employees child(ren)	109,855,889	90.01%	12,192,629	9.99%	122,048,518
Physically impaired information	109,909,307	92.77%	8,566,536	7.23%	118,475,843
Account No Login info	106,394,843	91.22%	10,241,205	8.78%	116,636,048
Employment date	106,410,883	91.98%	9,275,073	8.02%	115,685,956
Texas taxpayer ID	105,070,268	96.42%	3,903,253	3.58%	108,973,521
Educational background	90,012,380	87.16%	13,258,533	12.84%	103,270,913
Mothers maiden name	95,501,223	96.66%	3,298,220	3.34%	98,799,443
Divorce Decrees	91,924,826	96.05%	3,776,237	3.95%	95,701,063
Banking info	90,148,081	95.44%	4,309,884	4.56%	94,457,965
Emergency contact information	74,166,820	82.21%	16,047,206	17.79%	90,214,026
Immigration naturalization	77,865,379	89.01%	9,609,933	10.99%	87,475,312
Credit card debit card Number	79,525,640	90.92%	7,946,562	9.08%	87,472,202
Motor vehicle information	80,515,720	95.72%	3,601,746	4.28%	84,117,466
Substance abuse related information	69,922,925	88.47%	9,111,330	11.53%	79,034,255
Federal Employment ID Number	65,560,914	97.84%	1,446,281	2.16%	67,007,195
Criminal record	59,768,684	92.55%	4,810,833	7.45%	64,579,517
Federal Income Tax Information	48,158,302	88.28%	6,396,226	11.72%	54,554,528
Name of employees	46,089,453	86.49%	7,199,890	13.51%	53,289,343
Customer List	47,144,576	92.78%	3,666,473	7.22%	50,811,049
Photo	38,365,695	75.88%	12,196,570	24.12%	50,562,265
Loan Information	46,676,474	92.87%	3,585,980	7.13%	50,262,454
Passport Number	42,371,358	86.07%	6,859,918	13.93%	49,231,276
Business or personal financial statements	38,341,662	90.15%	4,190,275	9.85%	42,531,937
Lien Information	37,511,743	97.93%	791,211	2.07%	38,302,954
Handwriting Sample	34,676,605	92.35%	2,873,114	7.65%	37,549,719
Finger prints	35,454,489	96.44%	1,309,874	3.56%	36,764,363
Accounting Records	23,693,164	86.76%	3,616,625	13.24%	27,309,789
Wills	22,731,650	95.01%	1,193,610	4.99%	23,925,260
Credit history	21,043,717	91.27%	2,011,665	8.73%	23,055,382
Name and or Info of previous business owner	17,546,236	93.84%	1,151,500	6.16%	18,697,736
Bond Information	9,464,256	91.20%	912,993	8.80%	10,377,249
Tax violations	6,766,170	81.21%	1,565,814	18.79%	8,331,984
Tax Preparer Information	7,387,308	89.08%	905,887	10.92%	8,293,195
Retina or iris image	4,483,034	97.95%	94,000	2.05%	4,577,034
Other	99,958,898	92.68%	7,896,868	7.32%	107,855,766
Total	4,392,143,225	91.71%	396,926,162	8.29%	4,789,069,387

Exhibit B-4

Number and Percent of Contractors and Bidders Personally Identifiable Information by State Agencies and Institutions of Higher Education

as of January 1, 2010

Personally Identifiable information	State Agencies		Institutions of Higher Education		Total
	Number	Percent	Number	Percent	
Name	1,595,395	38.19%	2,582,052	61.81%	4,177,447
Social Security	1,485,866	37.84%	2,440,398	62.16%	3,926,264
Texas taxpayer ID	1,031,973	28.70%	2,564,217	71.30%	3,596,190
Qualification information	1,002,948	28.30%	2,540,469	71.70%	3,543,417
Federal Employment ID No	996,626	28.30%	2,525,539	71.70%	3,522,165
Business insurance information	907,372	26.34%	2,538,093	73.66%	3,445,465
Personal or Business Financial Statements	897,579	27.30%	2,390,514	72.70%	3,288,093
bid/contract/consultation amount	928,173	29.00%	2,272,916	71.00%	3,201,089
Personal email address	1,136,934	37.71%	1,877,717	62.29%	3,014,651
Contracts	840,581	27.91%	2,171,477	72.09%	3,012,058
Capacity information	886,150	29.74%	2,093,809	70.26%	2,979,959
Contract/bid/consultation history	788,731	26.54%	2,182,824	73.46%	2,971,555
Reference check	418,215	14.32%	2,502,140	85.68%	2,920,355
Personal cell Home phone Number	579,878	22.49%	1,998,336	77.51%	2,578,214
Bond Information	218,206	8.51%	2,344,961	91.49%	2,563,167
Driving Records	559,074	22.91%	1,881,641	77.09%	2,440,715
Tax violations	604,694	24.83%	1,830,726	75.17%	2,435,420
Federal Income Tax Information	662,119	27.56%	1,740,212	72.44%	2,402,331
Banking info	218,678	9.21%	2,156,412	90.79%	2,375,090
Home address	579,884	24.67%	1,770,607	75.33%	2,350,491
Photo	749,078	32.00%	1,591,524	68.00%	2,340,602
Handwriting Sample	650,574	28.43%	1,637,371	71.57%	2,287,945
Date of birth	558,836	25.94%	1,595,416	74.06%	2,154,252
Customer List	179,316	9.03%	1,806,614	90.97%	1,985,930
Immigration naturalization	92,057	4.86%	1,802,410	95.14%	1,894,467
Name and or Info of previous business owner	29,609	1.70%	1,709,207	98.30%	1,738,816
Name of employees	909,967	53.61%	787,422	46.39%	1,697,389
Birth place	85,110	5.08%	1,591,524	94.92%	1,676,634
Mother's maiden name	85,028	5.07%	1,591,524	94.93%	1,676,552
Passport No	82,016	4.93%	1,581,913	95.07%	1,663,929
Educational background	1,332,100	81.40%	304,345	18.60%	1,636,445
Credit card/debit card No	5,028	0.32%	1,581,913	99.68%	1,586,941
Criminal record	650,527	72.23%	250,046	27.77%	900,573
Employment data	678,935	96.08%	27,731	3.92%	706,666
Accounting Records	598,566	86.82%	90,885	13.18%	689,451
Finger prints	548,502	100.00%	0	0.00%	548,502
Emergency contact info	204,083	67.10%	100,054	32.90%	304,137
Credit history	95,166	46.10%	111,277	53.90%	206,443
Lien Information	13,150	6.59%	186,380	93.41%	199,530
Loan Information	71,778	46.08%	84,000	53.92%	155,778
Physically impaired info	80,000	100.00%	0	0.00%	80,000
Tax Preparer Information	5,178	12.18%	37,342	87.82%	42,520
Account No Login info	14,709	100.00%	0	0.00%	14,709
Motor vehicle info	10,028	100.00%	0	0.00%	10,028
Birth Certificates	0	0.00%	9,611	100.00%	9,611
Info about employees child(ren)	5,031	100.00%	0	0.00%	5,031
Info about employees spouse	5,028	100.00%	0	0.00%	5,028
Substance abuse related info	3,000	100.00%	0	0.00%	3,000
Other	231,321	56.08%	181,170	43.92%	412,491
Total	24,312,797	27.82%	63,064,739	72.18%	87,377,536

Appendix C:

Documents Pertaining to the Sale and Disclosure of Information under the Transportation Code

- Summary Table of Statutes Authorizing Release of Personally Identifiable Information
- Sample Documents Agencies Use to Collect Information:
 - DPS Application for Copy of Driver Record
 - TXDOT Peace Officer Crash Report
 - TXDOT Request for Copy of Crash Report
 - DMV Request for Texas Motor Vehicle Information
 - TPWD Merchandise for Sale
 - TPWD Application for License
 - TPWD Ownership/Lien Holder Information or Ownership History Report
- History of Provisions Governing the Protection of Motor Vehicle Records
- Summary of Provisions Authorizing Disclosure and Release of Information

Review of Selected Chapters

(Statutes that Release PII per guidelines of Transportation Code, Ch. 730)

Ch.	Title	Collects PII from:	Agency Responsible / Affected
Parks & Wildlife Code §11, §12, §31	<ul style="list-style-type: none"> - Organization - Powers and Duties Concerning Wildlife - Water Safety Act 	<ul style="list-style-type: none"> • Hunting/Fishing licenses • State Park entry and use Permits • Game Breeding/Falconry Permits • TP&W Magazine • Registration/Numbering of Boats, Boat Motors, Floating Cabins, Personal Watercraft 	➤ Parks & Wildlife Dept.
Trans Code, §501, §502	<ul style="list-style-type: none"> - Certificate of Title Act - Registration of Vehicles 	<ul style="list-style-type: none"> • Motor Vehicle Titles and Registration Records 	➤ Dept. of Motor Vehicles (Transferred as of 11/1/09 from TxDOT)
Trans Code, §521, §522	<ul style="list-style-type: none"> - Driver's License and Certificates - Commercial Driver's License Act 	<ul style="list-style-type: none"> • <i>Individual</i> Driver's License/Permit Applications • <i>Commercial</i> Driver's License/Permit applications 	➤ Dept. of Public Safety
Trans Code, §550	<ul style="list-style-type: none"> - Accidents and Accident Reports 	<ul style="list-style-type: none"> • Accident Reports (filed by operator or peace officer) • Autopsy Reports of Medical Examiners • Fatal Accident Reports of Justices of the Peace 	➤ Dept. of Transportation (Transferred as of 10/1/07 from DPS)
Trans Code, §730	<ul style="list-style-type: none"> - Motor Vehicle Records Disclosure Act 	<ul style="list-style-type: none"> • <i>Governs the Release of PII</i> information from all Motor Vehicle Records • Implements DPPA (1994) • Defines "PII" • Lists specific info permitted for release and who is qualified to request and receive that info • Establishes prohibitions of disclosure and use of improperly released info., resale or redisclosure of info., and penalties for same 	<ul style="list-style-type: none"> ➤ Dept. of Public Safety ➤ Dept. of Transportation ➤ Dept. of Motor Vehicles ➤ Parks & Wildlife Dept.

APPLICATION FOR COPY OF DRIVER RECORD**MAIL TO: Driver Records Bureau, Texas Department of Public Safety, Box 149246, Austin, TX 78714-9246**Make **CASHIER'S CHECK** or **MONEY ORDER** Payable To:
TEXAS DEPARTMENT OF PUBLIC SAFETYAny questions regarding the information on this form should be directed to
Customer Service at 512-424-2600. Allow 2-3 weeks for delivery.**Check Type of Record Desired****FEE**

<input type="checkbox"/> 1. Name - DOB - License Status - Latest Address.	\$ 4.00
<input type="checkbox"/> 2. Name - DOB - License Status - List of Accidents/Moving Violations in Record within Immediate Past 3 Year Period.	\$ 6.00
<input type="checkbox"/> 2A. CERTIFIED version of #2. This Record is Not Acceptable for DDC Course.	\$ 10.00
<input type="checkbox"/> 3. Name - DOB - License Status - List of ALL Accidents and Violations in Record. Furnished to Licensee ONLY.	\$ 7.00
<input type="checkbox"/> 3A. Certified version of #3. Furnished to Licensee ONLY and is Acceptable for DDC Course.	\$ 10.00
<input type="checkbox"/> Other: (Original Application, DWLS, etc.) _____	\$ _____ (If Required)

Mail Driver Record To: (Please Print or Type)

Requestor's Last Name Requestor's First Name

Street Address Texas Driver License Number

City State Zip Code Daytime Telephone Number (include area code)

If requesting on behalf of a business, organization, or other entity, please include the following:

Name of business, organization, entity, etc.

Your Title or Affiliation with above

Type of business, organization, etc. (i.e., insurance provider, towing company, private investigation, firm, etc.)

Information Requested On:

Texas Driver License Number MM/DD/YYYY _____
Date of Birth Suffix (SR., JR., etc.)

Last Name

First Name

Middle Name/Maiden Name

Individual's Written Consent For ONE TIME Release to Above Requestor

(Requestor, if you do not meet one of the exceptions listed on the back of this form, please be advised that without the written consent of the driver license/ID card holder, the record you receive will not include personal information.)

I, _____, hereby certify that I granted access on this one occasion to my Driver License/ID Card record, inclusive of the personal information (name, address, driver identification number, etc.) to _____.

Signature of License/ID

Card Holder or

Parent/Legal Guardian _____ Date _____

State and Federal Law Requires Requestors to Agree to the Following:

In requesting and using this information, I acknowledge that this disclosure is subject to the federal Driver's Privacy Protection Act (18 U.S.C. Section 2721 et seq.) and Texas Transportation Code Chapter 730. False statements or representations to obtain personal information pertaining to any individual from the DPS could result in the denial to release any driver record information to myself and the entity for which I made the request. Further, I understand that if I receive personal information as a result of this request, it may only be used for the stated purpose and I may only resell or redisclose the information pursuant to Texas Transportation Code §730.013. Violations of that section may result in a criminal charge with the possibility of a \$25,000 fine.

I certify that I have read and agree with the above conditions and that the information provided by me in this request is true and correct. If I am requesting this driver record on behalf of an entity, I also certify that I am authorized by that entity to make this request on their behalf. I also acknowledge that failure to abide by the provisions of this agreement and any state and federal privacy law can subject me to both criminal and civil penalties.

Signature of Requestor _____ Date _____

**If you are not requesting a copy of your own record or do not have the written consent of
DL/ID holder, you must provide the information requested on the reverse.**

Important Instructions - Read Carefully

The Texas Department of Public Safety may disclose personal information to a requestor without written consent of the DL/ID holder, on proof of their identity and a certification by the requestor that the use of the personal information is authorized under state and federal law and that the information will be used only for the purpose stated and in complete compliance with state and federal law.

You must meet one or more of the following exceptions if you do not have written consent of the DL/ID holder to be entitled to receive personal information on the above named individual. Please initial each category that applies to the requested driver record.

- _____ 1. For use in connection with any matter of (a) motor vehicle or motor vehicle operator safety; (b) motor vehicle theft; (c) motor vehicle emissions; (d) motor vehicle product alterations, recalls, or advisories; (e) performance monitoring of motor vehicles or motor vehicle dealers by a motor vehicle manufacturer; or (f) removal of nonowner records from the original owner records of a motor vehicle manufacturer to carry out the purposes of the Automobile Information Disclosure Act, the Anti Car Theft Act of 1992, the Clean Air Act, and any other statute or regulation enacted or adopted under or in relation to a law included in the above.
- _____ 2. For use by a government agency in carrying out its functions or a private entity acting on behalf of a government agency in carrying out its functions.
- _____ 3. For use in connection with a matter of (a) motor vehicle or motor vehicle operator safety; (b) motor vehicle theft; (c) motor vehicle product alterations, recalls, or advisories; (d) performance monitoring of motor vehicles, motor vehicle parts, or motor vehicle dealers; (e) motor vehicle market research activities, including survey research; or (f) removal of nonowner records from the original owner records of motor vehicle manufacturers.
- _____ 4. For use in the normal course of business by a legitimate business or an authorized agent of the business, but only to verify the accuracy of personal information submitted by the individual to the business or the authorized agent of the business and to obtain correct information if the submitted information is incorrect to prevent fraud by pursuing a legal remedy against, or recovering on a debt or security interest against the individual.
- _____ 5. For use in conjunction with a civil, criminal, administrative, or arbitral proceeding in any court or government agency or before any self regulatory body, including service of process, investigation in anticipation of litigation, execution or enforcement of a judgement or order, or under an order of any court.
- _____ 6. For use in research or in producing statistical reports, but only if the personal information is not published, redisclosed, or used to contact any individual.
- _____ 7. For use by an insurer or insurance support organization, or by a self insured entity, or an authorized agent of the entity, in connection with claims investigation activities, antifraud activities, rating or underwriting.
- _____ 8. For use in providing notice to an owner of a towed or impounded vehicle.
- _____ 9. For use by a licensed private investigator agency or licensed security service for a purpose permitted as stated on this page.
- _____ 10. For use by an employer or an authorized agent or insurer of the employer to obtain or verify information relating to a holder of a commercial driver license that is required under 49 U.S.C. Chapter 313.
- _____ 11. For use in connection with the operating of a private toll transportation facility.
- _____ 12. For use by a consumer-reporting agency as defined by the Fair Credit Reporting Act (15 U.S.C. §1681 et seq.) for a purpose permitted under the Act.
- _____ 13. For any other purpose specifically authorized by law that relates to the operation of a motor vehicle or to public safety.
Please state specific statutory authority _____
- _____ 14. For use in the preventing, detecting, or protecting against identity theft or other acts of fraud. The Department prior to release of personal information may require additional information.

This form is read by machine. Please print the numbers and letters as shown below:



1 2 3 4 5 6 7 8 9 0

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

☐ FATAL
 ☐ CMV INVOLVED
 ☐ SCHOOL BUS RELATED
 ☐ RAILROAD RELATED
 ☐ MEDICAL ADVISORY BOARD
 ☐ HIT AND RUN
 ☐ AMENDMENT/SUPPLEMENT


Texas Peace Officer's Crash Report

 Form CR-3
(Rev. 03/09)
Page 1 of 2

Submission of Crash Records: This report may be submitted via the CRIS Web Portal, electronically submitted via XML, or by mailing to the Texas Department of Transportation, Crash Records, PO Box 149349, Austin, TX 78714.
Questions? Call: 512/486-5780

PLACE WHERE CRASH OCCURRED COUNTY _____ CITY OR TOWN _____ IF CRASH WAS OUTSIDE CITY LIMITS <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> OF _____ INDICATE FROM NEAREST TOWN _____ MILES N S E W						LOC # _____ ORI # _____ TxDOT # _____	
ROAD ON WHICH CRASH OCCURRED BLOCK NUMBER _____ STREET OR ROAD NAME _____ ROUTE NUMBER OR STREET CODE _____ INTERSECTING STREET OR RR X'ING NUMBER BLOCK NUMBER _____ STREET OR ROAD NAME _____ ROUTE NUMBER OR STREET CODE _____ NOT AT INTERSECTION <input type="checkbox"/> FT. <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> OF _____ <input type="checkbox"/> MI. N S E W						CONSTRUCTION ZONE <input type="checkbox"/> YES <input type="checkbox"/> NO SPEED LIMIT _____ WORKERS PRESENT <input type="checkbox"/> YES <input type="checkbox"/> NO CONSTRUCTION ZONE <input type="checkbox"/> YES <input type="checkbox"/> NO SPEED LIMIT _____ WORKERS PRESENT <input type="checkbox"/> YES <input type="checkbox"/> NO <div style="border: 1px solid black; padding: 2px; width: fit-content;">MILEPOST</div> LATITUDE _____ LONGITUDE _____	
DATE OF CRASH _____ DAY OF WEEK _____ HOUR _____ MONTH _____ DAY _____ YEAR _____						<input type="checkbox"/> AM IF EXACTLY NOON <input type="checkbox"/> PM OR MIDNIGHT, SO STATE	
UNIT # <input type="checkbox"/> 1-MOTOR VEHICLE 4-PEDESTRIAN 7-NON-CONTACT 2-TRAIN 5-MOTORIZED CONVEYANCE 8-OTHER 3-PEDALCYCLIST 6-TOWED VIN # _____ YEAR _____ COLOR & _____ MODEL _____ BODY _____ LICENSE _____ MODEL _____ MAKE _____ NAME _____ STYLE _____ PLATE _____ YEAR _____ STATE _____ NUMBER _____						ALTERED VEHICLE HEIGHT <input type="checkbox"/> YES <input type="checkbox"/> NO	
DRIVER'S NAME _____ LAST _____ FIRST _____ M.I. _____ ADDRESS (STREET, CITY, STATE, ZIP) _____ PHONE NUMBER _____ DRIVER'S LICENSE _____ STATE _____ NUMBER _____ CLASS/TYPE _____ ENDORSEMENTS _____ RESTRICTIONS _____ DATE OF BIRTH _____ LICENSE STATUS _____ 1-VALID 2-NOT VALID 3-SUSPENDED/REVOKED 4-CANCELLED/DENIED 5-EXPIRED 6-UNKNOWN						DRIVER'S ETHNICITY _____ 1-WHITE 2-HISPANIC 3-BLACK 4-ASIAN 5-OTHER DRIVER'S SEX <input type="checkbox"/> MALE <input type="checkbox"/> FEMALE DRIVER'S OCCUPATION _____ POLICE, FIREFIGHTER, EMS, ON EMERGENCY <input type="checkbox"/> IF CHECKED, PLEASE EXPLAIN IN NARRATIVE	
TYPE OF ALCOHOL SPECIMEN TAKEN 1-BREATH 2-BLOOD 3-URINE 4-NONE 5-REFUSED TEST RESULTS _____ TYPE OF DRUG SPECIMEN TAKEN 1-BLOOD 2-URINE 3-NONE 4-REFUSED TEST RESULTS _____ DRUG CATEGORY 1. _____ 2. _____ <input type="checkbox"/> LESSEE <input type="checkbox"/> OWNER NAME (ALWAYS SHOW LESSEE IF LEASED, OTHERWISE SHOW OWNER) _____ ADDRESS (STREET, CITY, STATE, ZIP) _____ LIABILITY INSURANCE <input type="checkbox"/> YES <input type="checkbox"/> NO <input type="checkbox"/> EXP INSURANCE COMPANY _____ POLICY NUMBER _____ VEHICLE DAMAGE RATING _____							
UNIT # <input type="checkbox"/> 1-MOTOR VEHICLE 4-PEDESTRIAN 7-NON-CONTACT 2-TRAIN 5-MOTORIZED CONVEYANCE 8-OTHER 3-PEDALCYCLIST 6-TOWED VIN # _____ YEAR _____ COLOR & _____ MODEL _____ BODY _____ LICENSE _____ MODEL _____ MAKE _____ NAME _____ STYLE _____ PLATE _____ YEAR _____ STATE _____ NUMBER _____						ALTERED VEHICLE HEIGHT <input type="checkbox"/> YES <input type="checkbox"/> NO	
DRIVER'S NAME _____ LAST _____ FIRST _____ M.I. _____ ADDRESS (STREET, CITY, STATE, ZIP) _____ PHONE NUMBER _____ DRIVER'S LICENSE _____ STATE _____ NUMBER _____ CLASS/TYPE _____ ENDORSEMENTS _____ RESTRICTIONS _____ DATE OF BIRTH _____ LICENSE STATUS _____ 1-VALID 2-NOT VALID 3-SUSPENDED/REVOKED 4-CANCELLED/DENIED 5-EXPIRED 6-UNKNOWN						DRIVER'S ETHNICITY _____ 1-WHITE 2-HISPANIC 3-BLACK 4-ASIAN 5-OTHER DRIVER'S SEX <input type="checkbox"/> MALE <input type="checkbox"/> FEMALE DRIVER'S OCCUPATION _____ POLICE, FIREFIGHTER, EMS, ON EMERGENCY <input type="checkbox"/> IF CHECKED, PLEASE EXPLAIN IN NARRATIVE	
TYPE OF ALCOHOL SPECIMEN TAKEN 1-BREATH 2-BLOOD 3-URINE 4-NONE 5-REFUSED TEST RESULTS _____ TYPE OF DRUG SPECIMEN TAKEN 1-BLOOD 2-URINE 3-NONE 4-REFUSED TEST RESULTS _____ DRUG CATEGORY 1. _____ 2. _____ <input type="checkbox"/> LESSEE <input type="checkbox"/> OWNER NAME (ALWAYS SHOW LESSEE IF LEASED, OTHERWISE SHOW OWNER) _____ ADDRESS (STREET, CITY, STATE, ZIP) _____ LIABILITY INSURANCE <input type="checkbox"/> YES <input type="checkbox"/> NO <input type="checkbox"/> EXP INSURANCE COMPANY _____ POLICY NUMBER _____ VEHICLE DAMAGE RATING _____							
DAMAGE TO PROPERTY OTHER THAN VEHICLES _____ _____ _____							
OBJECT _____ NAME AND ADDRESS OF OWNER _____ FEET FROM CURB _____ \$ _____ DAMAGE ESTIMATE _____							
IN YOUR OPINION, DID THIS CRASH RESULT IN AT LEAST \$1,000.00 DAMAGE TO ANY ONE PERSON'S PROPERTY? <input type="checkbox"/> YES <input type="checkbox"/> NO							
CHARGES FILED NAME _____ CHARGE _____ CITATION # _____ NAME _____ CHARGE _____ CITATION # _____							
TIME NOTIFIED OF CRASH _____ DATE _____ HOUR _____ HOW _____ TIME ARRIVED AT SCENE _____ DATE _____ HOUR _____ DATE OF REPORT _____ TYPED OR PRINTED NAME OF INVESTIGATOR _____ ID # _____ AGENCY _____ DIST/AREA _____ REPORT COMPLETE <input type="checkbox"/> YES <input type="checkbox"/> NO							

REQUEST FOR COPY OF PEACE OFFICER'S CRASH REPORT

Mail To: Crash Records, Texas Department of Transportation, P.O. Box 12879, Austin, Texas 78711

Make check or M.O. payable to: Texas Department of Transportation

Questions? Call: 512/486-5780

CHECK TYPE OF SERVICE DESIRED:

☐ Copy of Peace Officer's Crash Report - \$6.00 each
 ☐ Certified Copy of Peace Officer's Crash Report - \$8.00 each

DATE OF REQUEST _____ **CLAIM OR POLICY NO.** _____

Transportation Code, Sec.550.065. **RELEASE OF CRASH REPORTS.** (b) Except as provided by Subsection (c), a crash report held by the department is privileged and for the confidential use of: the department; and an agency of the United States, this state, or a local government of this state having use for the report for crash prevention purposes. (c) allows release of a crash report on written request and payment of required fee: (4) a person who provides the department or law enforcement agency with two or more of the following: date of the crash; the name of any person involved; the specific location of the crash.

Please provide as accurate and complete information as possible.

CRASH DATE _____			
MONTH/DAY/YEAR			
CRASH LOCATION _____			
COUNTY	CITY	STREET OR HIGHWAY	
WAS ANYONE KILLED IN THE CRASH? _____ IF SO, NAME OF ONE DECEASED _____			
INVESTIGATING AGENCY AND/OR OFFICER'S NAME (if known) _____			

DRIVER'S FULL NAME	DRIVER INFORMATION (if available)		ADDRESS (if available)
	DATE OF BIRTH	TEXAS DL NUMBER	

PASSENGER'S FULL NAME	PEDESTRIAN or PEDALCYCLIST (if available)	ADDRESS (if available)

- ♦ Texas Statute allows the investigating officer 10 days in which to submit his/her report.
- ♦ Requests should not be submitted until at least 10 days after the crash date to allow time for receipt of the report.
- ♦ The Law also provides that if an officer's report is not on file when a request for a copy of such report is received, a certification to that effect will be provided in lieu of the copy and the fee will be retained for the certification.

Mail to _____

Mailing address _____

City _____ **State** _____ **Zip** _____

E-mail _____

Requested by _____ **Phone #** _____

FOR TxDOT USE ONLY

Date Received _____ I.D. No. _____ Clerk _____

☐ Report Sent Date _____

☐ Report not on file Date Searched _____

REQUEST FOR TEXAS MOTOR VEHICLE INFORMATION

I request that the Texas Department of Motor Vehicles (TxDMV), Vehicle Titles and Registration Division (VTR), furnish me with the information specified below that is contained in the vehicle title and registration records for the vehicle listed below.

Name of Requestor (Firm/Applicant) _____

Mailing Address _____

City _____ State _____ Zip Code _____ Daytime Phone (_____) _____

VEHICLE INFORMATION:

Current License Number

Expiration Year Of Plate

Year And Make Of Vehicle

Vehicle Identification Number

Title/Document Number

INFORMATION REQUESTED (Check the requested option):

OPTION 1. RECORD INQUIRIES:

- ☐ Title and registration verification of current motor vehicle record\$ 2.30
☐ Certified title and registration verification\$ 3.30
☐ Other (please describe the information requested) Fees vary

THE DEPARTMENT MAY ONLY RELEASE THE INFORMATION REQUESTED ABOVE IF:

(Check one, if applicable)

- ☐ (1) You are the subject (current recorded owner or lienholder) of the information contained in the record.
☐ (2) You certify that the intended use of the requested information is for the permitted use(s) as indicated on the back of this form. (If this option is chosen, back **MUST** be completed.)
☐ (3) You have written authorization (**MUST** be attached) from a person named in the record (previous owner, owner or lienholder) authorizing the department to release their personal information to you.

(NOTE: THE DEPARTMENT MAY ONLY RELEASE THE PERSONAL INFORMATION OF THE PERSON PROVIDING THE AUTHORIZATION.)

OPTION 2. TITLE HISTORIES (copies of Texas title transactions):

★ **THE DEPARTMENT MAY RELEASE A TITLE HISTORY ONLY** if the intended use of the title history is for a permitted use as indicated on the back. You **MUST** certify the permitted use(s) that applies to your request on the back of this form.

- ☐ Title history ★ \$ 5.75
☐ Certified title history ★ \$ 6.75

IN MAKING THIS REQUEST, I CERTIFY THAT:

1. This information is requested for a lawful and legitimate purpose and will be used in accordance with 18 U.S.C., §§2721-2725, and Texas Transportation Code, Chapter 730;
2. If the information is requested for a permitted use(s), I will only use the information for that permitted use; and
3. The personal information obtained pursuant to this request will not be used for marketing, solicitation or survey purposes; and
4. I have not been convicted of a violation of Transportation Code, Chapter 730, or violated a rule adopted by TxDOT relating to the terms and conditions for release of personal information from motor vehicle records.

I HEREBY CERTIFY THAT THE STATEMENTS CONTAINED HEREIN ARE TRUE AND CORRECT, TO THE BEST OF MY KNOWLEDGE.

SIGNATURE

PRINTED NAME

CURRENT GOVERNMENT-ISSUED PHOTO IDENTIFICATION NUMBER
(e.g., Driver's license, DPS ID, Military ID, passport)

STATE/AGENCY OF ID ISSUANCE

EXPIRATION DATE

WARNING: VIOLATION OF THIS AGREEMENT IS A CLASS A MISDEMEANOR. Texas Transportation Code, Chapter 730, provides that a person who makes a false statement or misrepresents their identity in order to obtain personal information from the department records commits a Class A misdemeanor, punishable by a fine not to exceed \$4,000, up to one year in jail or both.

This request must be submitted with cash, check cashier's check or money order in the amount indicated above. If you are mailing this request, cash is discouraged. Please remit your request to any VTR Regional Office or mail directly to the VEHICLE TITLES AND REGISTRATION DIVISION, TEXAS DEPARTMENT OF MOTOR VEHICLES, AUSTIN, TX 78779-0001.

PERMITTED USES

INITIAL (DO NOT CHECK ✓) ALL THAT APPLY IN THE SPACE PROVIDED:

USE OF THE REQUESTED PERSONAL INFORMATION WILL BE STRICTLY LIMITED TO:

- A.** Use by:
- ☐ (1) A government agency, including any court or law enforcement agency, in carrying out its functions; or
- ☐ (2) A private person or entity acting on behalf of a government agency in carrying out the functions of the agency.
- B.** Use in connection with any matter of:
- ☐ (1) Motor vehicle or motor vehicle operator safety.
- ☐ (2) Motor vehicle theft.
- ☐ (3) Motor vehicle emissions.
- ☐ (4) Motor vehicle product alterations, recalls or advisories.
- ☐ (5) Performance monitoring of motor vehicles, motor vehicle parts or motor vehicle dealers.
- ☐ (6) Motor vehicle market research activities, including survey research.
- ☐ (7) Removal of non-owner records from the original owner records of a motor vehicle manufacturer to carry out the purposes of the Automobile Information Disclosure Act, 15 U.S.C. §1231 et seq.; 49 U.S.C. Chapters 301, 305, 323, 325, 327, 329, and 331; the Anti Car Theft Act of 1992, 18 U.S.C. §§553, 981, 982, 2119, 2312, 2313, and 2322, 19 U.S.C. §§1646b and 1646c, and 42 U.S.C. §3750a et seq., all as amended; the Clean Air Act, 42 U.S.C. §7401 et seq., as amended.
- C.** ☐ Use in the normal course of business by a legitimate business or an authorized agent of the business, but only to verify the accuracy of personal information submitted by the individual to the business or the agent of the business; and if the information is not correct, to obtain the correct information, for the sole purpose of preventing fraud by, pursuing a legal remedy against, or recovering on a debt or security interest against the individual.
- D.** Use:
- ☐ (1) In conjunction with a civil, criminal, administrative or arbitral proceeding in any court or government agency or before any self-regulatory body, including service of process, investigation in anticipation of litigation, execution or enforcement of a judgment or order, or under an order of any court; or
- ☐ (2) For child support enforcement under Chapter 231, Family Code.
- E.** ☐ Use in research or in producing statistical reports, but only if the personal information is not published, redisclosed or used to contact any individual.
- F.** ☐ Use by an insurer or insurance support organization, or by a self-insured entity, or an authorized agent of the entity, in connection with claims investigation activities, antifraud activities, rating or underwriting.
- G.** ☐ Use in providing notice to an owner of a towed or impounded vehicle.
- H.** ☐ Use by a licensed private investigator agency or licensed security service for a purpose permitted under this section.
- I.** ☐ Use by an employer or an agent or insurer of the employer to obtain or verify information relating to a holder of a commercial driver's license that is required under 49 U.S.C. Chapter 313.
- J.** ☐ Use in connection with the operation of a private toll transportation facility.
- K.** ☐ Use for any other purpose specifically authorized by law that relates to the operation of a motor vehicle or to public safety. Please cite the specific law: _____
- _____
- _____

RESALE and REDISCLOSURE:

A person obtaining motor vehicle record information for any of these permitted uses may resell or redisclose the information **only** for these permitted uses, and must **maintain records for a period of not less than 5 years** of any person or entity that received the information and the permitted use for which it was obtained. The purchaser must also provide copies of those records to the department upon request. The information obtained as a result of this request may not be resold or redisclosed in the identical or substantially identical format as it is received from the department.



Merchandise for Sale

Texas Parks & Wildlife Expo

Life's Better Outside

Orders can be mailed to the address below with payment information or faxed (for credit card payments only) to:
ATTN: Expo Coordinator, (512) 389-8673.

<http://www.tpwd.state.tx.us/business/shop/featured>

Quantity	Expo/Life's Better Outside Merchandise Description	Size	Unit Cost	Total Cost
Subtotal				
Total Shipping*				
TOTAL				

***Shipping Notes: Allow 3 to 4 weeks for delivery.**

- T-Shirts, Caps, Cups, Water Bottles and Posters are \$2.00 shipping per item.
- Bumper Stickers are \$1.00 each for shipping. (*\$1.00 waived if additional merchandise is purchased.*)

****See Contact Information below for bulk orders (quantity greater than 10 each.)**

Please make checks payable to: Texas Parks & Wildlife Expo

Mail to: Texas Parks and Wildlife Department

Attn.: Expo

4200 Smith School Road

Austin, TX 78744

Name: _____

Mailing Address: _____

City: _____ **State:** _____ **Zip Code:** _____

Phone: () _____ **E-mail:** _____

Credit Card Number (MC/Visa only): _____ **Exp. Date:** _____

Name on Card: _____ **3-digit Security Code:** _____

Signature: _____

****Expo merchandise questions? Contact (512) 389-4361.**

How did you hear about our merchandise? _____

Texas Parks and Wildlife Department maintains the information collected through this form. With few exceptions, you are entitled to be informed about the information we collect. Under Sections 552.021 and 552.023 of the Texas Government Code, you are also entitled to receive and review the information. Under Section 559.004, you are also entitled to have this information corrected.

TPWD USE ONLY: License No. _____ Plate/ID No. _____



Texas Parks and Wildlife Department
4200 Smith School Road, Austin, TX 78744 (800) 792-1112

APPLICATION FOR COMMERCIAL CRAB FISHERMAN'S LICENSE

☐ Resident (338) – \$630

☐ Non-Resident (438) – \$2,520

Applicant Last Name _____ First Name _____

Drivers License: State _____ No. _____ Date of Birth _____

Social Security Number _____ Phone No. _____

Address _____

City _____ State _____ Zip _____

County of Residence _____

I understand that I may hold no more than three of these licenses and that only one set of plates may be on board a boat at any time the boat is used for commercial crabbing purposes. This license is currently valid and has not been previously transferred or sold. I am eligible for this license under the limited entry criteria established by TPWD. I understand that it is a crime to make a false statement on this form.

Applicant Signature _____ Date _____

Employee Witness _____ Office Code _____ Date _____

(initial) Original TPWD issued license proving eligibility was presented.

Must be notarized if not signed before a TPWD employee.

Before me, a notary public, on this day personally appeared _____, a person whose identity is known to me. After I administered an oath to him, upon his oath, he said he read the Application for a Commercial Crab Fisherman's License, and that the facts stated in it are within his personal knowledge, and are true and correct.

Signature of Applicant

SWORN TO AND SUBSCRIBED BEFORE ME by _____,

on this the _____ day of _____, 20____.

NOTARY PUBLIC, STATE OF TEXAS

Printed name of notary _____

My commission expires _____

Texas Parks and Wildlife Department maintains the information collected through this form. With few exceptions, you are entitled to be informed about the information we collect. Under Sections 552.021 and 552.023 of the Texas Government Code, you are also entitled to receive and review the information. Under Section 559.004, you are also entitled to have this information corrected. Please note that the customer information collected through this form, including name, address, and telephone number, is considered public and is subject to disclosure under 31 Tex. Admin. Code § 51.303. However, you may elect to exclude your information from disclosure by checking this box ☐.



Ownership/Lien Holder Information Printout Or Ownership History Report (PWD 763)

This form is used to:

- **Obtain a computer printout**, which provides the current owner/lien holder name, address, vessel/boat and/or outboard motor description. The form PWD 763 must be completed and submitted with appropriate fees to TPWD Headquarters in Austin, a TPWD local law enforcement office, or a participating County Tax Assessor-Collector office.
- **Obtain the History**, which provides a copy of all documents submitted for transactions on file for a vessel/boat and/or outboard motor. TPWD retains historical documentation for vessels and outboard motors for a period of 10 years. The form PWD 763 must be completed and submitted with appropriate fees to TPWD Headquarters in Austin.

Check if your request is for a vessel/boat, outboard motor or both. Complete multiple forms if you need information for more than one vessel/boat and one outboard motor.

☐ **Vessel/Boat Information:** Please complete each blank if possible.

TX #: _____ HIN/Serial#: _____
Make: _____ Year Built: _____
Owner of Record Name and Address: _____

☐ **Outboard Motor Information:** Please complete each blank if possible.

M# (if known): _____ MIN/Serial #: _____
Make: _____ Year Built: _____
Owner of Record Name and Address: _____

Select the type of information you are requesting on the vessel/boat and/or outboard motor.

☐ **Ownership/Lien Holder Information Printout – fee \$0.00** each vessel/boat or outboard motor request

I, the undersigned, hereby request the name and address of the owner, name and address of the lien holder (if recorded), vessel/boat registration expiration date, and record status information on the vessel/boat and/or outboard motor described above.

☐ **Ownership History Report – (See Fee Chart)** each vessel/boat or outboard motor request

I, the undersigned, hereby request the historical transaction information recorded for the vessel/boat and/or outboard motor described above.

Check one: ☐ Normal History, or ☐ Certified History (letter is provided for court purposes)

Fees:

Number of Ownership/Lien Holder Reports Requested: _____ x \$0 = \$ _____

Number of Ownership History Reports Requested: _____ x (See Fee Chart) _____

Total Amount Enclosed: \$ _____

I hereby certify that the TPWD vessel/boat and/or outboard motor record obtained will be used for lawful purposes.

WARNING: Falsifying information on documents is a punishable offense – Texas Penal Code Chapter 37, Section 37.10. Any person who knowingly makes a false entry in, or false alteration of a governmental record is guilty of a felony of the third degree, punishable by confinement in jail for any term of not more than 10 years or less than 2 years and punishable by a fine not to exceed \$10,000. I hereby certify that all statements in this document are true and correct to the best of my knowledge and belief.

Signature of Applicant/Requestor: _____ Date: _____
Print Name: _____
Business Name (if applicable): _____
Mail to Address: _____
City: _____ State: _____ Zip: _____
Daytime Phone Number: _____

Texas Parks and Wildlife Department maintains the information collected through this form. With few exceptions, you are entitled to be informed about the information we collect. Under Sections 552.021 and 552.023 of the Texas Government Code, you are also entitled to receive and review the information. Under Section 559.004, you are also entitled to have this information corrected.

Brief History of the Transportation Code Provisions Governing the Protection of Motor Vehicle and Driving Records

The Texas legislature enacted these Chapters under the Transportation Code that govern the protection of individual privacy with regards to motor vehicle and driver's license records. The information contained within these records, particularly driver license records, is highly sensitive when it comes to privacy. In addition to the basic information contained in the driver license itself, such as the holder's address, date of birth, photograph, and signature, the driver license records held by the Department of Public Safety ("DPS") contain personal information such as the individual's social security number, telephone number, and medical and disability status.

Transportation Code, Chapters 521 (*Driver's Licenses and Certificates*) and 522 (*Texas Commercial Driver's License Act*) were originally enacted in 1995¹ and established which records DPS must create and maintain, including driver license applications and records, and accident and conviction reports. They also mandate that license applicants furnish DPS with their social security numbers, which are collected principally for child support enforcement purposes.² These chapters regulate the release of these records to third parties. For example, Section 521.050 allows DPS to supply private purchasers with magnetic tapes containing the names, addresses, and dates of birth of all license holders that are contained in DPS' basic driver license record file if the purchaser certifies in writing that the purchaser is eligible to receive the information under Chapter 730 of the Transportation Code.³

Transportation Code, Chapter 730 (*Motor Vehicle Records Disclosure Act*) was enacted in 1997⁴ to implement the federal Driver's Privacy Protection Act of 1994 ("DPPA").⁵ The DPPA bars states and their employees from releasing information, including names, addresses, photographs, and telephone and social security numbers, from motor vehicle records, except as authorized by the individual or by law. These laws are meant to protect the interest of an individual's personal privacy by prohibiting the unauthorized disclosure and use of personal information contained in motor vehicle records.⁶ Under Chapter 730 of the Transportation Code, an agency may not disclose personal information about any person obtained by the agency in connection with a motor vehicle record, unless provided by other provisions of the law to the contrary.⁷ Violations of the redisclosure or resale provisions of this chapter is a Class A misdemeanor offense.⁸

The 77th Legislature passed House Bill 1544 in 2001, which introduced several important changes to the Transportation Code, including the following: a revised schedule of fees for the selling of personal information from the driver license database, opt-out choices for license holders, procedures for governing the resale or redisclosure of information, establishing a Class B misdemeanor offense for obtaining accident information for use in direct solicitation of business, and disclosure of information through the internet.⁹

The circumstances in which personally identifiable information ("PII") may be disclosed to eligible requesters include instances where the information is needed for identity verification;

¹ Acts 1995, 74th Leg., ch. 165, Sec. 1, eff. Sept. 1, 1995; Amended by: Acts 2005, 79th Leg., ch. 1108, Sec. 3, eff. Sept. 1, 2005

² Trans. Code, Title 7, §521.044

³ *Id* at §521.050

⁴ Acts 1997, 75th Leg., ch. 1187, Sec. 1, eff. Sept. 1, 1997

⁵ 18 U.S.C. 2721, et seq. (1994)

⁶ Trans. Code, Title 7, §730.002

⁷ *Id* at §730.004

⁸ *Id* at §730.015

⁹ Texas Legislature Online, *Window on "Bill Information" HB1544*. Available: <http://www.capitol.state.tx.us>.

civil, criminal, or administrative proceedings; law enforcement or official government purposes; and child support enforcement.¹⁰ [See *Appendix A* for a selected review regarding disclosure of various types of personal information.] Other sections of Chapter 730 of the Transportation Code contain provisions governing related issues, such as: (1) redisclosure of the personal information, (2) fees that can be collected for the release of personal information, and (3) the penalties incurred for false representation when personal information is requested.¹¹

¹⁰ *Id* at §730.007

¹¹ *Id* at §§730.011-015

Disclosure, Release, or Access to Certain PII under Transportation Code is ALLOWED to:

- **Individual License Holder** *(on receipt of written request with required info. and \$7 fee)* ¹
- **Dept. of Public Safety** *(who maintains the records at issue herein – also to carry out statutory duties)* ²
- **Other law enforcement agencies** *(establish identity of victim or conduct investigations)* ³
- **Tx. Parks & Wildlife Dept.** *(a license deputy issuing license, stamp, tag, permit)* ⁴
- **Tx. Attorney General or other state entity responsible for Child Support Enforcement** ⁵
- **Tx. Alcoholic Beverage Commission** *(for purpose of enforcing, complying with, or preventing commission of an offense under TABC code or rule)* ⁶
- **Election Officer** *(establishing identity of a voter)* ⁷
- **Tx. Dept. of Health** *(state emergency or epidemic - need for immunizations)* ⁸
- **Person such as a Merchant** *(for limited purpose of checking age prior to selling cigarettes/tobacco products)* ⁹
- **Employee or agent for Public School District or tax-exempt organization that sponsors a program for youth** *(screening individual who will work with or have access to children)* ¹⁰
- **Official of U.S., State, or political subdivision of State** *(for gov't. purposes only)* ¹¹
- **Chief Appraisers** from each appraisal district in the State *(determining eligibility of residence homestead exemption from ad valorem taxation)* ¹²
- **Current or prospective employers** of individuals employed or seeking employment as motor vehicle or railway locomotive operators *(records requests that comply with policies of National Driver Register)* ¹³
- **US Selective Service System** *(disclosure of SSN allowed if applicant consents to register for SSS at the time)* ¹⁴
- **Financial institution or business** *(only for purposes of identification verification of an individual or check verification at the point of sale for a purchase of a good or service by check)* ¹⁵
- **Executive or administrative head of a Maritime Facility or of a port, port authority, or navigation district may authorize** *(to identify individual and secure the facility or port – specific limitations of use)* ¹⁶
- **Hospital** *(to provide health care services to the individual; however, if the individual objects to collecting the information from their driver's license, the hospital must use an alternative method for collecting that info)* ¹⁷
- **State Office of Administrative Hearings, Municipal, County and State Courts** *(personal info contained within administrative appeal files, such as for driver's license suspensions, etc.)*

**** Note:** All of the information made available above is confidential and not subject to redisclosure under Public Information Act per Trans. Code, §521.126(h) **

¹ Trans. Code, Title 7, §521.047

² *Id.* at §521.126(d)(1)

³ *Id.* at §521.126(d)(2); Code of Criminal Procedure, Title 1, Ch. 2, Art. 2.12

⁴ *Id.* at §521.126(d)(3); Parks and Wildlife Code, Title 2, §12.702 and §12.703

⁵ *Id.* at §521.044(a)(1) and (a)(2)

⁶ *Id.* at §521.126(d)(4); Alcoholic Beverage Code, Title 4, §109.61

⁷ *Id.* at §521.126(d)(1); Election Code, Title 6, Ch. 63

⁸ *Id.* at §521.049(a)

⁹ *Id.* at §521.126(d)(6); Health & Safety Code, Title 2, Subtitle H, §161.0825

¹⁰ *Id.* at §521.126(d)(7); Internal Revenue Code (of 1986, as amended), §501(c)(3)

¹¹ *Id.* at §521.049(c)

¹² *Id.* at §521.049(d); Tax Code, Title 1, Subtitle C, §11.13

¹³ *Id.* at §521.056

¹⁴ *Id.* at §521.044(a)(3) and §521.147

¹⁵ *Id.* at §521.126(e); 31 USC §5312(a)(2)

¹⁶ *Id.* at §521.126(g); 46 USC §70101, et seq.; Texas Constitution, §52, Art. III or §59, Art. XVI

¹⁷ *Id.* at §521.126(i), (j) and (k); HIPAA of 1996 (Pub. L. No. 104-191)

Appendix D:

Comments

Summary of Comments from the Following Survey Instruments

- Information Technology/Security
- Personnel/Staff
- Employment Applications
- Clients/Students/Members
- Open Record
- Bidder/Contractor

Summary of Comments from the Information Technology/Security Survey Instrument

What issues, if any, present a significant challenge in protecting PII?

Technology security:

E-mail [or transfer] of confidential data containing PII to authorized recipients outside the agency or other state agencies via unsecured methods.
PII residing on mobile computing devices [(e.g. removable media, laptops, USB drive, etc.)].
Everchanging security risks [(e.g. risks associated with social networking)] that come with technology.
The encryption of PII on the data drives.
Outsourcing the data center services creates an additional risk for any PII data collected and stored by the agency.
Some legacy applications do not store data as securely as newly written application.

Work area security: No issues.

Employee security issues:

Ensuring staff awareness so that they know when they are handling PII and that their systems and procedures provided adequate protection.
The number of users that require access to PII data in a decentralized environment creates a challenge to ensure policies are understood and enforced.
Effective disciplinary action for insufficient adherence to PII policies.
Some employees make unauthorized local convenience copies of PII for various processes. Ensuring that copy is deleted requires diligence by the employee.
The myriad of laws and regulations surrounding the protection of personal and sensitive information, coupled with an increasing move towards transparency of government, make it difficult for the average worker to clearly identify what personal information requires protection, and under what specific circumstances.

Miscellaneous:

Budget is the greatest challenge in dealing with protecting PII data.
With attention focused on the protection of PII using automated tools & techniques, certain organizations struggle to first identify the amount of PII collected, created, used or shared within their automated environments. With the increased use of electronic dissemination of data, the protection of PII has become quite important to maintain public trust and confidence in an organization, to protect the reputation of an organization, and to protect against legal liability for an organization. [The] most significant challenge appears to be the sheer increase in opportunities for misuse that accompany round-the-clock processing and dissemination of PII.
Continued use of SSN as a primary identifier by state and federal agencies.
Although we protect and secure confidential data, once we send information outside of [the agency], we do not have control over how the information is used.

Budget:

Defining PII data and acquiring the resources to secure this information.
Requirements from state & federal entities to provide reports containing PII causes spread of organizational elements collecting, storing & transmitting PII. Cost of implementing 2-factor authentication.

Summary of Comments from the Information Technology/Security Survey Instrument

General comments:

Since we are a health organization, the vast majority of the Personal Identifiable Information is covered under our HIPAA Privacy and Security Policies.
We do not have a wireless network. We use IT Best Practices (sFTP) when transferring data outside the agency. We don't have a vulnerability testing policy, but conduct one annually. We don't have a patch management policy, but patch when notified by the vendors.
Re: Ques-13&14. All staff receive periodic mandatory training regarding the Importance of maintaining confidentiality of PII. Re: 7&12 ERS maintains security of PII but cannot control how outside entities/individuals collect and transmit PII or how used after properly released.
Regarding Q 14: The agency does periodically distribute security & IT newsletters with security reminders, program areas also distribute notices as well.
The agency is a participating agency in the Statewide Data Center consolidation project
Question 4 - the IT Division (ITD) does not currently conduct formalized training for staff dealing with PII data. The topic is addressed through ITD's monthly newsletter, staff meetings & by posting informational brochures.
Our policies are not specific to PII but cover confidential data; which includes PII.
Since we are a health organization, the vast majority of the Personal Identifiable Information is covered under our HIPAA Privacy and Security Policies.
Q. 1: new applications must go through a Change Control Board review prior to authorization to launch; part of the CCB checklist requires a response to how the application has been designed to protect PII. Q. 4&5: all IT/IS staff receive the same mandatory training that all agency employees receive regarding security in general & the appropriate handling of PII in particular. in addition, about 50% of IT staff are formally trained in application design so their knowledge of security in this area is above average.
Answers to q. 7-9 will improve once the new document management system is put in place.
The TSU IT division is five months into a complete overhaul where strategic plans & process are being documented and implemented. The TSU CIO with the assistance of key advisors is re-organizing the department to meet all regulatory & business requirements.
The policies & safeguards put in place are intended to protect confidential & sensitive info. PII, when exempt from disclosure under the Public Records Act, falls under the said definition. The survey was completed under that premise. Q2: the review frequency is determined by risk level associated with the safeguard objective Q3: see comments for Q2. review frequency depends on the specific safeguard objective & it varies from one safeguard to another.
Having direction from the state on how to handle PII with respect to mobile devices and wireless networks.
All employees are trained in PII & privacy issues during orientation, prior to starting work. Issues of safeguarding PII routinely come up in IT discussions & planning & every member of the IT staff is acutely aware of the need to protect & secure PII.
With the exception of personnel records, the THC does not regularly collect PII in any of its applications. Most of this is handled through hard copy, not through electronic applications.
Tthe SPB is on the Texas Legislative Council's computer network & that agency provides all IT security for the agency.
IT staff that has access to PII is limited to two FTEs with 10+ years tenure & one outside contractor with 7 years tenure; we are keenly aware of these issues.
Qs 4, 5, 7-16 are n/a as the logical management of the PII data is the responsibility of the agencies that own/manage the data. Physical security for the PII data that resides on agency servers in the consolidated data centers is managed by the DCS contractor, IBM.
Q-1: no written policy exists at this time; however, the IT departments do follow "TAC 202 and industry standards & practices for safeguarding PII.

Summary of Comments from the Information Technology/Security Survey Instrument

We would like to be able to work with the CPA to reduce the use of employee SSNs in favor of an employee ID number.
The agency's security policies address protection of all information assets but most are not specific to PII.
Our agency shares IT personnel with other Health Professions Council (HPC) agencies and they are employed by HPC due to our MOU with the HPC. It is incumbent upon HPC to ensure that the IT personnel is properly and regularly trained. It has not been an issue.
The agency does not have any IT personnel on staff; however, the TFSC does contract with for all of its IT needs.
The agency operates a program that collects and maintains PII for core functions. Information is collected only for performance of statutory mandates.
Securing financial resources to protect data; securing management commitment to protect PII.
As stated above, no PII is collected or maintained in an electronic format on the agency's IT systems.
The Dept does not handle very much PII data. PII is either handled by the physical file system or is available in the Department database which is secured by authentication level security. Physical security is in place for the building and server/network specialist office.
Our database of applicants/registrants is maintained by DIR. They would do any security/testing of system. Employees use login ID & password to access system. Our computers are on TCEQ servers & they do regular backups/testing. We use login ID & password to access.
Q-14: we will be posting information in a common area to remind staff about the importance of the security of PII.
The IT Division is not stewards of all PII data. Data that resides somewhere other than our servers is less secure.
Regarding Q 5, training is supplied upon hiring and when new policies are changed or created.
The Office of Court Administration handles all our IT.
Laws and regulations struggle to keep up with creative and financially-motivated criminals who find new ways to abuse PII. Texas should take a proactive approach by protecting PII "by default" and only disclosing PII in exempted situation, rather than the reverse.
We treat all of our info with high regard and do not share PII.

Summary of Comments Generated from the Personnel/Staff Survey Instrument

Most recent request [not to share PII]

A new employee submitted the standard agency form indicating that no PII be released.
All employees are asked to fill form HR 181.
Disclosure form completed at NEO request not to share SSN.
Employees have a restraining order against a former spouse and requested that no information to be shared.
Forms allow students to restrict student directory info or release of educational records.
New hire indicated "yes. I want my personal info to be confidential" on Tarleton's Employee Personal Data Form.
Not to share salary information.
One employee requested not to share her PII to her ex-boyfriend.
Personal danger.
We ask new hires to fill out a form to allow the release of home address, SSN, and phone number.

What issues, if any, present a significant challenge in protecting PII?

Technology security:

Changing technology.
Current systems require PII to complete a process such as SSN or payroll, bank routing number for deposit, address and phone number for job applicants.

Work area security:

The biggest challenge is controlling & monitoring the incidental PII that some departments may collect for a specific reason & do not control the storage or the security of the info.
The same key opens all offices and storage space is very limited.

Open Records requests:

Having to disclosure information in response to a PIA request that most people in the workforce do not have to disclose.
Media requests.
The fact that a requestor upon requesting PII has a presumption per the Public Information Act that the info is open to them, this forces the agency to spend time to request an AG.

Employee /education security issues:

Access by CPA staff to PII. Password protected, but individual judgment is relied upon to maintain confidentiality.
Available material on what is or is not PII.
Training staff.
Continue to train employees and enforce the policies.
Employee turnover.
Giving access to the information to staff who may not need the info to do their jobs.

Budget: No issues.

Summary of Comments Generated from the Personnel/Staff Survey Instrument

Miscellaneous:

Many Texas state agencies we do business with require disclosure of SSN.
Natural disaster, criminal activity.
Our manual process has its own problems.
our personnel files are in hard copy form.
Record retention requirements.
Texas Identification Number is based on SSN, all employees are paid using that number.

General comments:

All HR personnel are aware that improper use of PII will result not only in termination but probably prosecution.
Data security is included in employee's ethics training.
I believe PII is to be protected. It must be so up front in law.
Internal Database is maintained by the Office of VPAA.
No PII is given out.
Still too much paper documentation being used and stored.
Tarleton employees are required to complete an annual training on handling PII. The training is called "information security awareness."
TDI provides all record storage and maintenance.
The Tx Public Info Act requires that we release (upon written request) certain info on our employees (state employees) who have not specifically requested that we not release their personal info (name, address & DOB).
UTHSCT only collects info that is required by state or federal government. For benefit purposes, the info was vary from employee to employee depending upon their elections. Info is only collected after the employee has accepted the job offer.
We protect PII to the fullest reasonably possible.

Summary of Comments Generated from the Employment Applications Survey Instrument

Most recent request [not to share PII]

Applicant who had a DUI asked that we not share that info. w/anyone.
New employee electing to have certain types of info. w/held from general public under TPIA.
Asked, due to certain injunction order on ex spouse, not to reveal address or phone number.
Internal applicants have a completed PIA election form on file, most requesting that certain info. not be released. Sometimes applicants request that no notice be provided to supervisor that they have applied for a position.
A candidate who was not selected for employment asked HR to remove his SSN from our files.

What issues, if any, present a significant challenge in protecting PII?

Technology security:

Security of electronic submissions through internet.
Current systems requiring Pii to complete a process such as bank routing numbers (direct deposit), home address and telephone number (for job applicants).
The fact that it is a manual paper process is a challenge. SSNs are collected and stored as apart of the application and that is a challenge.
Network is backed up weekly and quarterly. Electronic copies remain on backup tapes for far longer than their retention period.
Dependent systems that are not integrated and require data to be entered several times to process new hires.

Work area security: No responses.

Employee /education security issues:

Copying applications to share with interview panel and being sure all copies are returned to HR and shredded.
Applications may be mailed, faxed or emailed; the information floats around and may be handled by individuals not properly trained to protect confidential info.

Budget: No issues.

General comments:

Challenges of protecting Pii has significantly been reduced since State app was revised to omit the SSN.
While apps are processed centrally at our Austin HQ, they are frequently dropped off at local offices and mailed/faxed to HQ. There are numerous opportunities for information to be seen by unauthorized eyes before it gets to HR.
Electronic application system only allows qualified applications to be transferred to the hiring managers. Hiring managers are trained on proper hiring procedures and the importance of confidentiality.
Most PII is not collected until selected candidate accepts job offer and comes to HR to begin processing new hire paperwork.

Agency's/institution's policy in dealing with copies of employment applications distributed to screening and/or interviewing panels:

Summary of Comments Generated from the Employment Applications Survey Instrument

No Policy.
No copies of apps are made for screening or interviewing panels. The panels are allowed to look at the application and return it to Human Resources.
Hiring supervisors are instructed by Human Resources to collect all copies of applications from the search committee members and return them to Human Resources for shredding or to personally shred them in the hiring department.
Copies of applications, interview questions, notes and all other interviewing and selection information shall be returned to Human Resources for storage and destruction per records retention.
Guest user access to the applicant database is given to each committee member. Limited Pii, such as home address, home phone, work history, criminal information, and education information, is available to Guest Users.
All copies of employment applications are returned to Human Resources.
Each committee member must sign a confidentiality agreement which speaks to how to appropriately handle applicant docs, etc.
Electronic only

Summary of Comments Generated from Client/Student/Member Survey Instruments

Issues presenting significant challenge in protecting PII:

Technology security

Movement toward electronic sharing of medical records may represent a significant challenge in protecting PII data.
Database compromise - hackers. Printed info not picked up at the copier. Faxed documents, info.
On-going outside threats to access computer information systems.
Tighter controls on info security classes & how much info can be accessed based on security classes.
Transmission of encrypted PII data from one authorized entity to another authorized entity, especially if neither entity shares the same encryption standards.
Changing technology, hacking capabilities, no physical control over info that has been properly distributed to outside entities.
Electronic files only as secure as our best firewall.
Some legacy applications do not store data as securely as newly written applications. Notwithstanding, the database where the PII is stored have significant controls in place to limit, control & audit access to data.
Continually changing electronic standards & security methods is always a concern. Changes to the TAC that seek to enhance security but which frustrate users because information sharing and centralization within the institution is diminished.
Data backup.
E-mail.
Changing technology available to the general public.
The worst form is the paper copy of PII.
Electronic attacks on the institution's servers.
Unsecure email resource.
Lack of funding for converting hard copy documents to electronic for more secure processing and storage.
Credit/debit card data & bank account info require special safeguards such as firewalls to prevent unauthorized access of electronic databases.
Our largest challenge is that our e-mail is not secure, however it is the best way to share info with a group. We are all held accountable for sharing info and for maintain records of those reports and e-mail is a convenient way to do so in most cases. We will implement electronic records on 6/1/10.

Work area security

Other challenges include: 1) securing of documents containing PII in an accounting area where such a large volume of paper (example: vouchers, vendor maintenance documents) included PII. 2) Receiving faxed documents such as direct deposit applications or verification of SSN for vendor maintenance by fax on machines shared by various staff in the division.
Applications submitted by fax & mail by customers contain credit card/debit care #s. These applications are not stored in secured cabinets and these numbers are within view of agency employees who enter office as well as contractors. This is unavoidable due to the need to process applications.
Carelessness in leaving data unsecured.
Shared fax machines, central mail room.
Check in, check out, and treatment areas are not sound proof so other patients/students may overhear someone sharing their PII (appropriately) with health center staff; this is a major challenge for all health care facilities, particularly ones that were built prior to the HIPAA era (early 2000s). Design of clinic & other patient spaces.
Having adequate storage areas for the information.
Lack of private & secure offices.
Current "open" design of reception area.

Open records requests

The open records law is very broad & trying to understand the exceptions is difficult.
Open records requests.
The fact that the Public Information Act exists. Just because we're a publicly-funded institution does not, in my opinion, give people outside our institution the right to obtain information from our database.
The main challenge we face in this area is dealing with state legal entities who request info and we have to decide on how much info should be shared and still protect the confidentiality of the client.

Summary of Comments Generated from Client/Student/Member Survey Instruments

Employee security issues:

Only issue that poses potential challenge is that our care mgrs conduct off-site patient visits and carry patient info on their person and there is always possibility of that info being lost or stolen.
Access of data to employees.
While it has gotten better, some client agencies use the individual's SSN as a personal identifier on numerous reports, putting a tremendous burden on staff to catch every SSN when redacting, particularly since much of our disclosure is to pro se inmates.
At this point, an inadequate amount of staff to maintain records. We are trying to fill positions now.
When walking away from PC while at work, users should always lock down PC.
It is important to continually remind staff of security best practices. People are the weakest links in securing PII and training is the key.
Training of personnel regarding protecting PII data.
Widespread education of employees with regard to student and protected medical data. We do very good job of this however.
This department would benefit from training to protect the safety & security of PII data.
Keeping all employees in a large organization, such as Texas State, diligent in protecting PII data & continually informing them of policies and procedures is challenging.
Scholarship applications are distributed to faculty and staff members as paper copies.

Miscellaneous:

Many of the loan and grant cycles are 30 years. Securing information for such an extended period of time all poses risks to information accessing/integrity.
Current payment processing (USAS, TINS) requires use of SSNs and other PII (name, address) in order to make payments.
Payroll data collected is required by federal regs including the Copeland Act and Davis-Bacon Act & related acts.
Law enforcement constantly wants us to release info to them and don't understand why we cannot accommodate their requests.
Training and policy are key in maintaining and protecting PI data.
Too many people have access to too much info w/o demonstrating a "need to know". For example, the "universal" EIS/Compass data feed include date of birth and visa/citizenship status fields that most recipients of the feed probably don't need. The data feed is convenient, but is distributed very broadly.
Info received & requested by fed government - Dept of Education & Dept of Health & Human Services such as credit card info on entrance interview form.
Records retention period.
Educating public about protecting their data and then using that education consistently.
Since this info was considered public info before the law was changed & was provided to third party requestors, we find third parties have kept and still maintain PII provided before the law was changed. Some of this info will appear on the internet sites.
Our biggest challenge is what can happen after we give a copy of a parental authorization form to a student on the way down to make a purchase. The student can lose the paperwork, which has sensitive info on it, including CC #s and expiration dates in most cases.
Requests from private business interests such as credit card companies, banks, apartment complexes, etc.
At times, international students send personal credit card #s, bank statements and scanned passport photos via email. We tell them NOT to send the info this way - to fax it instead - but they often send the info this way. After it is printed and filed or shredded, electronic copy of email is deleted.
Primarily we rely on the respondent to ship hard copies of patient records. We have no control over how secure that info is until it reaches us. Any use of third-party shipper is a significant challenge to secure PII data.

Summary of Comments Generated from Client/Student/Member Survey Instruments

Most recent request not to share PII:

Licensee was being stalked by ex-spouse & requested that her address not be released.
Unknown. These requests come to the local eligibility offices on a daily basis & most certainly when information is received from the client that they are victims of family violence situations.
Wish to remain anonymous.
Less than 20-students complete form to withhold directory info and it is maintained in their academic file.
Some donors ask that their gifts remain anonymous.
Requested withholding of directory info.
Students request that directory info (name, phone #, email) be hidden in our student system via a website. Non-directory info (grades, medical, etc.) is always protected by FERPA regs.
Clients request travel info such as the Tx State Travel Guide. They request that their name not be provided to others which we comply with by marking their record private.
Subscriber requested removal from mailing list sales and we marked record as private.
"Please do not allow anyone my name and address."
License applicants can request TxRC not to disclose their personal info to public - TxRC notes in database not to disclose.
HRC 81.006(4) requires a registry of interpreters to be maintained and made available. Many interpreters do not want to be included in the registry.
Request to keep home address confidential.
Phone numbers, mailing address and business location addresses.
There are a few instances where we may received documents stamped "confidential". All info submitted to CPA is subject to requirements of Tx Gov't Code 552 (PIA).
Every state employee must advise whether certain personal info (SSn, home address, family member names) may be shared.
Constituent requested that email address not be shared with other email recipients.
Typical example is a consumer who does not want their PII shared with the business about which they complained for fear of retaliation.
These requests are made as a result of domestic violence reports, communicated by electronic transmission through the federal & state case registries, or by completed hard copy of non-disclosure.
Can't recall specifics but probably party would have requested that the info be maintained confidential unless the court ordered otherwise.
Client did not want anyone to see personal & business info of any kind. Request was granted and respected.
A person was going through a divorce and requested information could not be shared.
Requests by members to not receive any additional affinity mailings from outside vendors on behalf of the Alumni Association.
FERPA waivers are only to individuals identified by the student; usually the parents for academic information.
As published in our college catalog, we identify information that is considered "public information." as further noted, if a student so chooses to have that withheld, they need only submit a written request.
Requests not to share health info are often made verbally between the student/patient & the health care provider and may not be documented in: release of health info requires patient/student consent.
Request from parents of clinical patients who request that we do not send out medical reports regarding their children to anyone.
FERPA allows institutions to identify certain items to be considered as Directory Info and disclosed to anyone. We provide students the opportunity to tell us that they DO NOT want any info released.
These requests are a result of our Family Educational Rights privacy Act (FERPA) compliance policy and are completed at the beginning of each matriculation cycle. The request is in place until revoked in writing.
Patients routinely sign asking that PII not be shared.
Most people leave their SSN off the form. I cannot think of a specific request we have received not to share PII.
A sole proprietorship was not comfortable giving her SSN in addition to her EIN even though the info was required for TINS.
In 2006 we received a request from an individual concerned that we were requesting SSNs as part of our registration process. He wanted to ensure that we were not selling the data to a 3rd-party vendor.
Parents requesting info regarding their child's medical condition. Students wanting to know who has sexually transmitted diseases. Students wanting to know if their partner has received treatment.
Student declined to share their info with a family member while experiencing a mental health crisis after being transported to

Summary of Comments Generated from Client/Student/Member Survey Instruments

the hospital by police dept.
Patient records were subpoenaed. Patient requested that they not be released. University attorney consulted & treatment records were not released.
The requests originate in the Registrar's database. When a student who has requested privacy via the Registrar's Office graduates from the university, we also honor that request within the alumni database.
Requests sought to prevent the sharing of crime info with third parties.
Plaintiff, an unemployment benefits recipient, contacted the AAG representing the agency and requested that all agency documents bearing his SSN and date of birth be redacted before being filed in court.
Requested that their info be destroyed if they didn't get position.
Someone who was a potential stalking victim asked that her photo not be put on the web.
Student stipulated that they did not want their disability info shared with their parent.
A student did not want Student Judicial Programs to share data in regard to his judicial case with his mother.
Student did not want his name published in the Commencement program.
Faculty requests not to release personal phone number to students.
An alumni asked not to share his information.
Students estranged from parents.
Client in litigation and requested the agency to refrain from sharing personal information that was contained in public records.
Did not want a business address to appear with his business information on the web site.
A client did not want his name attached to a response to a staff report.
Court reporters requested not to have their personal information released.
Student was hesitant about me speaking with instructors concerning accommodations for his disability.
A staff physician did not want his PII shared with anyone other than other attending physicians.
An individual refused to participate in a survey.
One who reported illegal activity requested not be release his PII.
Students not wanting their financial aid awards discussed with their families.
Law provides victims of sexual assault to use a pseudonym name for protection of their PII.
Students want to keep resume confidential.
Business requested not to release information regarding business concept.
Peace officers' PII are confidential.
Postdoctoral fellow did not want forwarding information publicly disclosed at the end of his educational appointment.
We offer patients the use of alias names and a confidentiality flag that prompts for a required personal ID number that the patient sets up to access information or it is not released. Exception: filing medical claims.
To list gift as anonymous.
Disclosing information about a disability to faculty member(s).

General comments:

#7 - PII must be shared with the Comptroller to establish a Texas Identification # (TIN) and make payments. PII may be shared with other agencies for problem resolution regarding shared recipients. Misrouted monetary receipts may be forwarded to other agencies.
A large majority of our "clients" are corporations or associations and no personal info is collected other than a contact name, with the exception of home phone numbers that might be given in lieu of a business phone number on an application for a Residential Marina.
Access to personal data is limited to 2 staff members within our division. In the last 12 years we have not been asked to share any client or camper data with any outside agency.
All Air Force personnel receive annual training on Information Security. This training covers protection of Privacy Act info as well as protection and handling of classified and other sensitive info.
All clinical & business records (PHI & PII) are stored & released according to HIPPA regulations & UT record storage & IT security guidelines & practices. This record was reconstructed following an earlier submittal in which the content was not printed. Content is similar but not exactly identical to that document.
All info collected by this division is investigative by nature and is not subject to open records request under statute.
All PII data are stored on the mainframe or server systems.
Annually the College trains approx 200 front-line employees who deal with students & their PII on recognizing the potential

Summary of Comments Generated from Client/Student/Member Survey Instruments

of identity theft & dealing with the risks of keeping the PII confidential.
Answers reflected on survey are compilation of data related to statewide accounting systems including USAS, USPS, HRIS, SPRS, SPA & TINS. No individual requests received; however, transactions can be marked confidential by agencies.
As a training organization, we must meet the demands of the training sponsor or certifying agency. Some state agencies have moved away from SSNs (as we have) but some state agencies still require us to collect and store SSNs.
Badge ID files include employee and consultant/contractor pictures. Parking permit files include employee & consultant/contractor vehicle license #s.
Because we offer mental health services, we follow the strict guidelines provided by the Texas LPC legal code. Therefore all of our procedures are within state guidelines.
Credit card numbers are not stored at the institution but by the payment processing provider at a hosted location.
Documents are scanned by employees with no security or HIPAA training.
Drivers license numbers & credit card numbers are collected but not retained when accepting payments from students.
Emphasis on security of PII will continue during future meetings and/or professional development sessions.
Enrollment Management (the division/program submitting this survey) includes the offices of Admissions, Registrar and Student Financial Aid & Scholarships.
Extremely confident in the personnel who have the ability to process, enter or view PII.
Faculty and staff are generally very sensitive to the disclosure of PII as this has been traditionally emphasized in the culture of us as a health science center.
For sole proprietors (vendors) we use a prefix of "2", a system generated check digit and a 3-digit mail code to make up their full 14 digit tax ID # for making payment. Imbedded in this number is the recipient's SSN.
Forwarding addresses are collected if the person that has a mailbox will be leaving the university if they want to.
General consulting on health care related activities.
Hard copies of forms that parents fill out about their children are boxed annually and hand-carried to Records Retention for 6 years.
I believe that in general we are very secure in making sure personal information isn't distributed from our office. However, we could definitely stand to have postings about FERPA and other such laws so that way any new work study students or employees can have them as reminders.
Info gathered for open faculty positions in the department. Most info listed on applicatns CVs or resumes.
Info is not collected from patients. Data received is collected from hospital/clinic billing data. When data is accessed for benchmarking purposes there are levels of security that do not allow for data to be drilled down at a patient level except for the submitting hospitals/clinic.
Information collected from client is strictly to extend credit for our services & maintain their accounts. All applications are stored securely. We are in the process of storing these electronically with limited access. Client information is not shared with any other agencies.
Information is not collected from patients. Data is entered by staff at the hospital conducting the utilization review.
Medical records, physically impaired information, electronic image of face is not required, but often submitted as additional documentation for admission files.
Most of the info collected by the University Police Department is outside the "normal" university channels. The accessibility of the info is governed at a federal, state or university level. Conflicting policies are resolved through review by Police Command staff & other appropriate parties.
On question 3, the types of information the agency collects is related to cancer prevention and research grant proposals & contracts for cancer prevention & research grant awards. We actually collect business addresses, email addresses & telephone numbers versus home or personal information in these categories.
Our students PII is kept in a locked cabinet & locked office when the office is closed. During open hours there is someone in this office.
The individuals served by the agency guardianship are wards of a court which has determined they are incapacitated and unable to manage either their personal affairs or their financial affairs. The information gathered and maintained by the program on these individuals is vital to the performance of the duties as guardian. this information is also presented to the court prior to the judge making his or her decision and elements of it is available to the report annually as appropriate and in compliance with state laws.
The only information we publish is the business contact for approved materials. As such this info is probably not classified as PII. It is published as a service to the company and the construction industry.
This is the first time in my 4 years at the university that I've heard concern expressed regarding PII on departmental sites. We need instruction on best practices for protecting users' PII.

Summary of Comments Generated from Client/Student/Member Survey Instruments

This program completely redacts any identifying patient, provider & hospital info. The program is conducted in a confidential manner so that peer review can be conducted in a fair & unbiased fashion.
Training is priority.
The licensing offices release address and phone numbers to vet clinics and the Association's office. Vet clinics use info for billing purposes. Associations request info for racing related purposes.
The center takes head shot portraits of many faculty and administrators. Staff members are photographed rarely although they may be in relation to a story, and students are photographed occasionally for news or marketing. We also take photos of people in crowds in public settings, working in labs, classrooms, etc.
We have policies protecting PII, we train our staff, have audit trails in place to monitor activity and only collect specific information for business purposes. The above list in item 3 is not collected on all patients receiving medical services, only pertinent information needed for their services require certain data elements.
We provide the reservation form and the parental authorization form as a service to our customers. We couldn't operation w/o credit card sales in the store. On-line sales credit card info is never in our possession.
Would like to continue receiving updates on best practices to secure PII. Use of latest technologies to identify potential risks.

Summary of Comments Generated from Open Record Survey Instrument

Most recent request [not to share PII]

Open Records Request from Advanced Financial Strategies requested a list of all employees' names, home and work addresses, and Date of Birth. 270 employees chose to withhold their addresses.
Individual did not want address available on licensing database via internet.
A party to a case did not want the opinion involving her case available by Google search of her name.
The Texas State Employee Union has requested the names, addresses and personal identification numbers of all university faculty and staff. Those numbers were provided even though there are some security issues.
A licensee requested that we refrain from listing the licensee's address and phone number on our Website.
Licensees and complainants requesting that their PII be kept confidential.
An individual was victim of domestic violence, changed her name but did not go through the OAG protection program.
Licensee complained that they are receiving too much "junk mail" that is a result of our agency selling names and addresses.
A request was submitted for all applications responsive to a posted job position. The employee hired for the position had a request on file not to provide her PII data.
An employee anticipated that a fellow employee might request their personnel information.
Licensees may request that their home address/phone number be made confidential. The licensee must then provide an alternate address/phone number on record.
Individual did not want their name attached to a response to a staff report.
A request from a court reporter that her personal information not be disclosed.
Staff and trustees are given the opportunity to withhold certain PII named in the Disclosure Election forms filed under Gov't Code Section 552.024.
Request was made by a faculty member to not provide colleagues' phone numbers which were included in responsive documents.
Request was made for background investigations from OPM for Homeland Security.
Students have asked for their directory info to be withheld under FERPA and employees have asked that their home addresses and telephone numbers be withheld.
Students w/privacy flag in self-serve acct. Students per semester have set privacy flags restricting release of certain PII. Request for student directory info by College Board Selection - Requested current student name, address, phone, university assigned email & classification. Students with privacy flags were removed.
We had one person submitting a bid proposal ask that we not share their SSN or address.
We receive numerous requests to protect personally identifying info that is public under current state law, such as taxpayers' business addresses and phone numbers.
Female employee did not want her ex-husband (who she claimed physically abused her) to gain access to her current address or other info.

What issues, if any, present a significant challenge in protecting PII?

Technology security:

Not having exclusions of internal identification numbers can present problems. While SSNs and DLNs may be protected, the internal IDs are the first step necessary to get access to computer system and there is room for abuse.
I would think it would be difficult to protect a lot of PII data due to so much information being computerized and in electronic format. With so much being scanned into computers and computer hackers, it would be difficult to keep all the PII information safe.

Summary of Comments Generated from Open Record Survey Instrument

As new technologies are deployed, they must be constantly re-evaluated for data protection effectiveness. Intrusions from outside our systems present the most significant challenges in protecting PII. Protecting PII against evolving modern technology is a constant challenge.
Ever-changing technology for storage and transmission of information.

Work area security:

No issues.

Open Records requests:

The most significant challenge for this agency is that individuals (inmates, family members, etc) include their own personal info (i.e. medical info) when lodging a complaint against a facility under our purview. The public may not be aware that some of that info may be subject to open record.
Cannot have control over everything that is considered public information. Definition is very broad and must rely on others to assist in collecting & protecting information.
None, the agency only releases name and addresses for most open record requests.
Once we release data in response to a public information request, a request for disclosure in litigation, or transferred to another agency, we have no control over its security.
Most PII is not confidential and therefore must be released pursuant to the PIA. The only PII that is easily withheld is driver's license numbers and social security numbers.
We sometimes received information containing PII that we don't ask for or seek to collect from the parties to our cases. This leaves us in possession of the information, which may be buried within voluminous material that we don't have the capacity to review closely before making public. We have a rule directing parties to redact such information before filing it with us, but the parties do not always comply with this requirement. As of Sept. 2010, filings in our cases will be available to the public via the internet, which will increase the importance of excluding unnecessary PII from the documents filed with our agency.
There is no exception under the Public Information Act to protect dates of birth. Also, there are no exceptions to protect personal information (home address, phone, etc) of non-employees, i.e. individuals that apply for positions and are not hired.

Employee security issues:

Changes and turnover in staffing require ongoing training and familiarization.
--

Budget:

The agency's biggest challenge is its budget.

Miscellaneous:

If an employee fails to declare his/her PII as confidential, the information is subject to public access. In order to protect PII, this information should only be available to the public if authorized in writing by the employee. (Opt-In vs. Opt-Out)
Students comprise most of the PII data that this institution maintains. As such, the students themselves often fail to protect their own PII, sometimes posting this information on social networking websites.
The most significant challenge is in ensuring that small vendors do not provide personal information when responding to procurement requests and that if the information is received it is appropriately

Summary of Comments Generated from Open Record Survey Instrument

marked as confidential.
Balancing transparency with protecting individual identity, home addresses, phone numbers, dates of birth and other common law privacy items such as income for mandatory customers of state agency services and voluntary recipients of services from state agencies.

Most recent requests not to share PII:

Bidder asked for its financial statement to be confidential.
Bidders asked not to share SSN, and home address.
Clients do not want to share PII.
Company responding to request for proposals stated that their solicitation was confidential.
Not sharing proprietary information.
REP response stamped confidential on certain documents like resume, etc.
Request to redact financial info in bid/award package requested in open records request.
The resumes of individual offered within a proposal to perform the 'statement of work' were stamped 'confidential' and each contained personal information about the worker.
Unsuccessful bidder requests for awarded bidders' complete package.
Winning respondent wanted the entire proposal considered 'confidential'.

General comments:

Our agency's costs associated with providing information under the TPIA far exceed any amounts we receive through the cost recovery process.
Agency provides routine training regarding the Texas Open Records Act.
All info has limited access by employees in the areas/divisions that it resides.
Certain info is required to be collected for Federal tax reporting purposes.
Every effort is taken to keep confidential information safe and secure.
It must be so up front in law without trying an agency's hands each and every time to request an AG's Open Records Opinion.
No personal info is given out.
Some data are only requested for specific types of procurements.
SSN and Phone numbers are required if it is a sole proprietorship.
Staff receives periodic mandatory training regarding PII.
Technology landscape is constantly changing.
The agency rarely goes out for bids.
The majority of contracts executed by the agency are open enrollment contracts.
Various bidder info for large purchases is gathered by another agency that is part of the system.
We are a small agency and rarely go out for bids, we don't have a database/files.
We are a small agency and utilize the same vendors for the majority of our purchases or services required.

Summary of Comments Generated from Bidder/Contractor Survey Instrument

What issues, if any, present a significant challenge in protecting PII?

Technology security:

It could be a problem if agency's servers are not secure.
One of the PII data is encrypted.
Removable computer devices such as CD, DVD, etc.
Remember to purge electronic records in accordance with records retention schedule.
Some contractors cannot initiate encrypted messages to the state.
TINS requires a SSN or EIN, so they are collected and stored electronically in accounting system.

Work area security:

Lack of secure space.
Location of stored records and unable to secure storage equipment.
Maintenance of paper files.
Locking the cabinets is an important security issue.

Open Records requests:

One challenge is responding to PIA requests.
Open Records as a State agency -Public Information Act-Texas Government Code, Chapter 552.

Employee security issues:

Some are sensitive about how PII is managed. The perception is that not all internal parties treat PII in a sense manner.
Training new employees about PII.

Miscellaneous:

The info required by the government with the W-9 can present challenges for some PII data.
The state park division conducts its own RFPs for state park concessions with no participation by TPWD. It appears that these concession RFPs request unnecessary information.

Most recent requests not to share PII:

Bidder asked for its financial statement to be confidential.
Bidders asked not to share SSN, and home address.
Clients do not want to share PII.
Company responding to request for proposals stated that their solicitation was confidential.
Not sharing proprietary information
RFP response stamped confidential on certain documents like resume, etc.
Request to redact financial info in bid/award package requested in open records request.
The resumes of individual offered within a proposal to perform the 'statement of work' were stamped 'Confidential' and each contained personal information about the worker.
Unsuccessful bidder requests for awarded bidders' complete package.
Winning respondent wanted the entire proposal considered 'confidential'.

Summary of Comments Generated from Bidder/Contractor Survey Instrument

General comments:

Agency provides routine training regarding the Texas Open Records Act.
All info has limited access by employees in the areas/divisions that it resides.
Certain info is required to be collected for Federal tax reporting purposes.
Every effort is taken to keep confidential information safe and secure.
It must be so up front in law without trying an agency's hands each and every time to request an AG's Open Records Opinion.
No personal info is given out.
Some data are only requested for specific types of procurements.
SSN and Phone numbers are required if it is a sole proprietorship.
Staff receives periodic mandatory training regarding PII.
Technology landscape is constantly changing.
The agency rarely goes out for bids.
The majority of contracts executed by the agency are open enrollment contracts.
Various bidder info for large purchases is gathered by another agency that is part of the system.
We are a small agency and rarely go out for bids; we don't have a database/files.
We are a small agency and utilize the same vendors for the majority of our purchases or services required.

Appendix E:

Survey Instruments and Totals

Sample Instruments and Totals for the Following Survey Types:

- Information Technology/Security
- Personnel/Staff
- Employment Applications
- Clients/Students/Members
- Open Record
- Bidder/Contractor

Information Security/Information Technology Questionnaire

Agency/Institution: 104 state agencies/58 IHEs

Completed by: _____ Telephone No.: _____

E-mail Address: _____

Ques-1 Are policies in place which address the following: (check all that apply)

- 149 ☐ Proper use, handling, storage, disclosure and destruction of personally identifiable information (PII)
- 147 ☐ Physical safeguards protecting PII in applications
- 144 ☐ Safeguards for protecting PII in databases
- 114 ☐ Security requirements for wireless networks (if they can be used to access PII)
- 134 ☐ Vulnerability and/or penetration testing of systems/applications/databases containing PII
- 156 ☐ Data wiping/sanitization/destruction (for media containing PII)
- 128 ☐ Use and protection of removable media (for storing/transporting PII)
- 128 ☐ Secure transfer of PII data outside of the organization
- 144 ☐ Patch management of applications, systems and databases (on which PII is processed/stored/transferred)
- 28 ☐ Other _____

Ques-2 Are safeguards reviewed for effectiveness on a regular basis?

- 24 ☐ No (if **NO**, go to Question 4)
- 147 ☐ Yes

Ques-3 If **YES**, How frequently are the safeguards reviewed?

- 43 ☐ More than once per year
- 76 ☐ Annually (at least once per year)
- 23 ☐ Bi-Annually (at least once every 2 years)
- 5 ☐ Every 3-4 years
- 0 ☐ Every 5 or more years

Ques-4 Approximately what percentage of IT/IS staff dealing with PII data are trained on the proper use, handling and storage of Personally Identifiable Information (PII)? 0 to 100%

Ques-5 How frequently are staff trained in handling PII?

- 94 ☐ Annually (at least once per year)
- 32 ☐ Bi-Annually (at least once every two years)
- 26 ☐ Every 3 years or longer
- 15 ☐ Never

Ques-6 Are vulnerability and/or penetration tests performed against applications, systems and databases containing PII?

27 ☐ No (If **NO**, go to **Ques-7**)

142 ☐ Yes

If **YES**, how frequently are these tests performed?

29 ☐ More than once a year

97 ☐ Annually (at least once per year)

16 ☐ Bi-Annually (at least once every two years)

3 ☐ Every 3-4 years

1 ☐ Every 5 or more years

We would like to know your opinion in reference to the following topics. How do you rate the safety and security of PII in your division/program by marking [1] as the LOWEST (not at all secure) and [10] as the HIGHEST (very secure):

	Not Secure					Very Secure				
	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]	[10]
Ques-7 In reference to the way in which PII is collected/received ?	[1]	[0]	[0]	[1]	[3]	[12]	[26]	[58]	[43]	[25]
Ques-8 In reference to the way in which PII is stored/maintained ?	[0]	[1]	[1]	[1]	[2]	[8]	[22]	[52]	[51]	[31]
Ques-9 In reference to the way in which PII is transmitted to authorized recipients?	[0]	[1]	[1]	[2]	[0]	[8]	[21]	[45]	[54]	[36]
Ques-10 In reference to the way in which PII is handled by staff responsible for managing it?	[1]	[0]	[1]	[0]	[1]	[12]	[20]	[59]	[45]	[30]
Ques-11 In reference to requests for information from outside the agency ?	[0]	[1]	[0]	[2]	[1]	[4]	[23]	[35]	[57]	[44]
Ques-12 In reference to sharing with other agencies/divisions?	[0]	[1]	[0]	[0]	[0]	[8]	[16]	[45]	[56]	[39]
Ques-13 Is the subject of security and/or privacy of PII discussed in weekly or monthly meetings?	[103] Yes					[51] No	[15] Don't Know			
Ques-14 Are there postings or announcements in the work area reminding staff of the need for safety/security of PII?	[55] Yes					[105] No	[8] Don't Know			
Ques-15 In your view, do personnel receive adequate training in assuring safety and security of PII?	[124] Yes					[30] No	[16] Don't Know			
Ques-16 In your view, what issues, if any, present a significant challenge in protecting PII data?										

Personnel/Staff Questionnaire

Agency/Institution: 100 state agencies/57 IHEs

Completed by: _____ Telephone No.: _____

E-mail: _____

Ques-1 What was the total number of agency/institution employees (part-time and full-time) as of Jan. 1, 2010? 385,237

Ques-2 What was the total number of agency/institution former employees (part-time and full-time) that you had in your files/databases as of Jan. 1, 2010? 1,506,195

Ques-3 Which of the following items does your Agency/institution collect from Employees/Staff? (Select all that apply)

- 166 ☐ Name (First and Last)
- 165 ☐ Social Security No.
- 164 ☐ Date of birth
- 33 ☐ Birth Place
- 165 ☐ Home Address
- 166 ☐ Employment Data (hire date, pay, etc.)
- 17 ☐ Mother's Maiden Name
- 98 ☐ Personal E-mail Address
- 94 ☐ Passport No.
- 162 ☐ Personal Cell/Home Phone No.
- 15 ☐ Texas Taxpayer Identification
- 4 ☐ Credit Card/Debit Card No.
- 143 ☐ Banking Info. (Acct No., Routing No. etc)
- 23 ☐ Finger Prints
- 15 ☐ Handwriting/Sample Handwriting
- 89 ☐ Medical Information
- 79 ☐ Physically Impaired Information
- 92 ☐ Photo (Electronic Image of face)
- 0 ☐ Retina or Iris Image
- 98 ☐ Criminal Record
- 25 ☐ Substance Abuse Related Information
- 158 ☐ Educational Background (Schools, degrees, etc.)
- 144 ☐ Immigration, naturalization & citizenship
- 110 ☐ Information about the Employee's Spouse
- 108 ☐ Information about the Employee's Child(ren)
- 79 ☐ Prior Performance Evaluations
- 12 ☐ Credit History
- 85 ☐ Motor Vehicle Info. (lic. plate, reg., etc.)
- 10 ☐ Tax Violations
- 28 ☐ Account No./Login Information
- 8 ☐ Business or Personal Financial Statements
- 13 ☐ Loan Information
- 159 ☐ Emergency Contact Information
- 110 ☐ Driving Records (driver's license, accidents etc.)
- 123 ☐ Outside Employment
- 69 ☐ Birth Certificate
- 28 ☐ Other (please list): _____

19 [] Other (please list): _____

8 [] Other (please list): _____

Ques-4 Of all the Personally identifiable Information (PII) data which you have checked above, which information could you cease to collect without being detrimental to the functioning of your agency, division or program? Please identify them in the following space by corresponding letters such as k, n, aa, ... etc.

personal e-mail (25); personal phone (11); electronic image of face (9); outside employment (8); motor vehicle information (7); information about employee's spouse (7); information about employee's children (6); emergency contact (6); DOB (4); passport no./driving record/prior performance reviews (3)

Ques-5 Do you ask your employees to sign an agreement allowing the disclosure of Personally Identifiable Information (PII)?

[115] Yes [53] No (*If NO*, go to Ques-7)

If YES, please include a copy of the agreement with this questionnaire.

Ques-6 *If Yes*, is signing the agreement mandatory or voluntary?

[70] Mandatory [46] Voluntary

Ques-7 What is your agency's/institution's policy for sharing employees' PII? (Check all that apply)

63 [] There is a specific written policy against sharing employees' PII

70 [] There are general guidelines for sharing employees' PII

0 [] Employees' PII is sold to private parties

13 [] Employees' PII is sold to or shared with other governmental entities

63 [] Other (Please explain) _____

Ques-8 What is the agency's/institution's procedure for dealing with PII relating to former employees? (check all that apply)

49 [] Destroy/purge the information

117 [] Keep information in central location

14 [] Keep in the former employee's division

37 [] Keep all information in an electronic/database format

48 [] Keep certain information in an electronic/database format (list types of information): _____

42 [] Other (Please explain) _____

Ques-9 Have you received any request(s) from an individual not to share his/her PII?

[92] Yes [76] No (**If NO** , go to **Ques-12**)

Ques-10 **If YES**, approximately, how many during the last 2 Years? 32,726

Ques-11 Would you please briefly explain the most recent request?

We would like to know your opinion in reference to the following topics. How do rate the safety and security of PII in your division/program by marking [1] as the LOWEST (not at all secure) and [10] as the HIGHEST (very secure):

	Not Secure							Very Secure		
	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]	[10]
Ques-12 In reference to the way in which PII is collected/received ?	[0]	[0]	[0]	[3]	[2]	[5]	[7]	[34]	[70]	[47]
Ques-13 In reference to the way in which PII is stored/maintained ?	[0]	[0]	[1]	[2]	[3]	[5]	[10]	[26]	[61]	[60]
Ques-14 In reference to the way in which PII is transmitted to authorized recipients?	[0]	[0]	[0]	[2]	[4]	[6]	[6]	[37]	[61]	[50]
Ques-15 In reference to the way in which PII is handled by staff responsible for managing it?	[0]	[0]	[0]	[2]	[1]	[1]	[10]	[26]	[72]	[56]
Ques-16 In reference to requests for information from outside the agency ?	[0]	[0]	[0]	[0]	[3]	[1]	[9]	[24]	[60]	[64]
Ques-17 In reference to sharing with other agencies/ divisions?	[0]	[0]	[0]	[0]	[2]	[0]	[9]	[24]	[65]	[62]
Ques-18 Is the subject of security and/or privacy of PII discussed in weekly or monthly meetings?	[53] Yes [96] No [18] Don't Know									
Ques-19 Are there postings or announcements in the work area reminding staff of the need for safety/security of PII?	[34] Yes [119] No [14] Don't Know									
Ques-20 In your view, do personnel receive adequate training in assuring safety and security of PII?	[129] Yes [30] No [8] Don't Know									

In your view, what issues, if any, present a significant challenge in protecting PII data?

Comments

We wish to thank you for taking the time to assist us in gathering this information. We will provide you with a link to the report when it has been completed and published.

Employment Applications Questionnaire

Agency/Institution: 103 State Agencies/61 IHEs

Completed by: _____ Telephone No. _____

E-mail Address: _____

Ques-1 In what format does your agency/institution receive employment applications? (check all that apply)

138 ☐ Electronic

114 ☐ Hard copies

91 ☐ Fax

11 ☐ Other _____

Ques-2 Approximately how many employment applications are received by your agency/institution per month? 220,368

Ques-3 What is the agency's/institution's procedure for dealing with application documents which do not result in hiring? (please check all that apply)

35 ☐ Destroy the applications **(including copies)**

74 ☐ Archive the applications

22 ☐ Keep the applications at the division/program level which posted the original position

72 ☐ Keep the applications in an electronic/database format

25 ☐ Keep some information from the application in an electronic/database format

52 ☐ Other (please explain) _____

Ques-4 How long after hiring are the unwanted applications destroyed/
deleted? 1-6

[0] Days

[0] Weeks

[4] Months

[143] Years

Ques-5 Do the divisions/programs return the unwanted applications to HR?

[99] Yes [37] No [19] Sometimes

Ques-6 Do managers/administrators receive training in dealing with unwanted applications?

[113] Yes [45] No

Ques-7 Does the agency/institution have a follow-up policy for tracking the unwanted applications?

[75] Yes [83] No

Ques-8 Which of the following items are kept in an electronic/hard copy format? (Check all that apply)

- 170 ☐ Name (First and/or Last)
- 107 ☐ Social Security No.
- 110 ☐ Date of Birth
- 11 ☐ Birth Place
- 163 ☐ Home Address
- 165 ☐ Home Phone No.
- 153 ☐ Work Phone No.
- 160 ☐ Employment Data (date of employment, salary, etc.)
- 50 ☐ Immigration, naturalization & citizenship
- 14 ☐ Birth Certificate
- 6 ☐ Mother's Maiden Name
- 145 ☐ E-mail Address
- 107 ☐ Driver's License No.
- 5 ☐ Finger Prints
- 13 ☐ Handwriting/Sample Handwriting
- 20 ☐ Medical Information
- 20 ☐ Physically Impaired Information
- 14 ☐ Photo (Electronic Image of face)
- 85 ☐ Background/reference check
- 58 ☐ Criminal Record
- 15 ☐ Substance Abuse Related Information
- 149 ☐ Educational Information
- 29 ☐ Other (Please explain) _____

Ques-9 What is your agency's/institution's policy for sharing Personally Identifiable Information (PII) gathered from employment applicants? (Check all that apply)

- 35 ☐ There is a written policy against sharing the information
- 106 ☐ There is a clear guideline required by HR for dealing with applicant information
- 1 ☐ Applicant information is sold to private parties
- 58 ☐ Other (Please explain) _____

Ques-10 Please briefly explain the agency's/institution's policy in dealing with copies of employment applications distributed to screening and/or interviewing panels: _____

Ques-11 Have you received any request(s) from an individual not to share his/her application PII?

[13] Yes [159] No (**If NO**, go to **Ques-14**)

Ques-12 **If YES**, approximately, how many during the last 2 Years? 1,134

Ques-13 Would you please briefly explain the most recent request? _____

We would like to know your opinion in reference to the following topics. How do you rate the safety and security of PII in your division/program by marking [1] as the LOWEST (not at all secure) and [10] as the HIGHEST (very secure):

		Not Secure					Very Secure				
		[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]	[10]
Ques-14	In reference to the way in which PII is collected/received ?	[0]	[1]	[0]	[1]	[3]	[13]	[6]	[28]	[66]	[53]
Ques-15	In reference to the way in which PII is stored/ maintained ?	[0]	[0]	[0]	[2]	[3]	[3]	[11]	[23]	[70]	[59]
Ques-16	In reference to the way in which PII is transmitted to authorized recipients?	[0]	[0]	[1]	[2]	[3]	[7]	[8]	[31]	[67]	[51]
Ques-17	In reference to the way in which PII is handled by staff responsible for managing it?	[0]	[0]	[0]	[2]	[2]	[2]	[12]	[23]	[74]	[56]
Ques-18	In reference to requests for information from outside the agency ?	[0]	[0]	[0]	[0]	[1]	[2]	[4]	[23]	[54]	[78]
Ques-19	In reference to sharing with other agencies/ divisions?	[0]	[0]	[0]	[0]	[1]	[1]	[6]	[21]	[58]	[75]
Ques-20	Is the subject of security and/or privacy of PII discussed in weekly or monthly meetings?	[50] Yes					[97] No	[23]	Don't Know		
Ques-21	Are there postings or announcements in the work area reminding staff of the need for safety/security of PII?	[34] Yes					[122] No	[14]	Don't Know		
Ques-22	In your view, do personnel receive adequate training in assuring safety and security of PII?	[137] Yes					[20] No	[13]	Don't Know		
Ques-23	In your view, what issues, if any, present a significant challenge in protecting PII data from employment applicants?										

Agency No. _____ Quesi Division/Program _____

Clients/Students/Patients/Members Questionnaire

Agency: _____

Completed by: _____

Telephone No. _____

E-mail: _____

Ques-1 Information entered in this questionnaire is in reference to:

- 387 Clients/Service recipients
- 476 Students
- 121 Patients
- 129 Members
- 404 Other (please explain)

Ques-2 Approximately how many clients/students/patients/members were included in your files and/or databases in FY 2009? Number **352,069,104**

Ques-3 What type of information is collected from the above category(ies) by your division/program? (Please check all that apply)

- 1,110 ☐ Name (First, Last, Middle)
- 550 ☐ Social Security Number
- 700 ☐ Date of Birth
- 228 ☐ Birth Place
- 868 ☐ Home Address
- 326 ☐ Employment
- 78 ☐ Mother's Name
- 680 ☐ Personal E-mail Address
- 113 ☐ Passport No.
- 805 ☐ Personal E-mail Address
- 137 ☐ Texas Driver's License
- 138 ☐ Credit Card
- 151 ☐ Banking Info (e.g., Account/Routing No.)
- 50 ☐ Finger Prints
- 68 ☐ Medical Records
- 326 ☐ Medical Records
- 185 ☐ Physically
- 146 ☐ Electronic
- 3 ☐ Retina or Iris
- 172 ☐ Criminal
- 138 ☐ Substance
- 454 ☐ Educ Background (schools, degrees, etc.)
- 257 ☐ I-9
- 223 ☐ Information
- 194 ☐ Information
- 44 ☐ Credit History

- 90 ☐ Motor Vehicle Info (license plate, reg., etc.)
- 34 ☐ Tax Violations
- 210 ☐ Account No.
- 148 ☐ Personal or Business Financial
- 243 ☐ Names of employees
- 97 ☐ Accounting Records
- 131 ☐ Contracts
- 63 ☐ Customer List
- 73 ☐ Loan Information
- 127 ☐ Federal Income Tax Information
- 47 ☐ Lien Information
- 43 ☐ Bond Information
- 98 ☐ Federal Employment ID No.
- 49 ☐ Tax Preparer Information
- 47 ☐ Name and/or Info. of previous
- 32 ☐ Wills
- 99 ☐ Divorce Decrees
- 115 ☐ Birth
- 115 ☐ Death Certificates
- 300 ☐ Emergency Contact
- 199 ☐ Driving Records (driver's license, accident info., etc.)
- 309 ☐ Other (Please specify)

Ques-4 Of all the Personally Identifiable Information (PII) data which you have checked above, which information could you cease to collect without being detrimental to the functioning of your agency, division or program? Please identify them in the following space by corresponding letters such as k, n, aa, ... etc.

SSN (38); personal e-mail (31); personal phone (25); DOB (20); birthplace (13); emergency contact (13); educational background (11); employment data (10); electronic image of face (9); driving record (7)

Ques-5 Do you ask your clients to sign an agreement which would allow the disclosure of personally identifiable information?

[241] Yes [892] No (*If NO* , go to **Ques-7**)

If YES, please attach a copy of the agreement with this questionnaire.

Ques-6 *If Yes* , is signing the agreement mandatory or voluntary?

[105] Mandatory [137] Voluntary

Ques-7 What is your division/program's policy for sharing clients' PII? (Check all that apply)

- 491 ☐ There is a specific written policy against sharing the clients' PII
- 372 ☐ There are general guidelines for sharing PII
- 22 ☐ Clients' PII is sold to private parties
- 9 ☐ Clients' PII is sold to other governmental entities
- 166 ☐ Clients' PII is shared with other governmental entities
- 463 ☐ Other (Please explain) _____

Ques-8 What is your division's/program's procedure for dealing with PII relating to clients who are no longer receiving services? (check all that apply)

352 ☐ Destroy/purge the information

456 ☐ Keep the information in a central location

185 ☐ Keep in the division from which the client received services

443 ☐ Keep all information in an electronic/database format

223 ☐ Keep certain information in an electronic/database format (list types of information): _____

308 ☐ Other (Please explain) _____

Ques-9 Have you received any request(s) from an individual not to share his/her PII?

[199] Yes [933] No (*If NO*, go to **Ques-12**)

Ques-10 **If YES**, approximately, how many during the last 2 Years? 1,337,371

Ques-11 Would you please briefly explain the most recent request?

We would like to know your opinion in reference to the following topics. How do you rate the safety and security of PII in your division/program by marking [1] as the LOWEST (not at all secure) and [10] as the HIGHEST (very secure):

		Not Secure					Very Secure				
		[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]	[10]
Ques-12	In reference to the way in which it is collected/received?	6	1	11	14	39	60	111	252	276	348
Ques-13	In reference to the way in which it is stored/maintained?	7	2	3	5	32	34	84	173	384	395
Ques-14	In reference to the way in which PII is transmitted to	9	0	2	5	22	36	70	209	326	408
Ques-15	In reference to the way in which PII is handled	5	0	4	2	20	24	66	222	353	422
Ques-16	In reference to requests for information from outside the agency ?	4	0	3	3	17	11	36	174	282	510
Ques-17	In reference to sharing with other agencies/divisions?	3	0	2	3	16	12	52	181	288	478

Ques-18	Is the subject of security and/or privacy of PII discussed in weekly or monthly meetings?	Yes 509	No 491	Don't know 123
---------	---	------------	-----------	-------------------

Ques-19	Are there postings or announcements in the work area reminding staff of the need for safety/security of PII?	Yes 387	No 646	Don't know 88
---------	--	------------	-----------	------------------

Ques-20	In your view, do personnel in your program area receive adequate training in assuring safety and security of PII?	Yes 949	No 73	Don't know 84
---------	---	------------	----------	------------------

Ques-21 In your view, what issues, if any, present a significant challenge in protecting PII data?

Open Records Questionnaire

Agency/Institution: 191 responses from 105 State Agencies and 57 IHEs

Completed by: _____ Telephone No.: _____

E-mail: _____

Ques-1 How many written requests for information did your agency receive during FY 2009? 1,070,991

Ques-2 Of those requests, what percentage included **Personally Identifiable Information (PII)** (i.e., name, address, date of birth, etc.)? 0% to 100% - total = 712,293 requests

Ques-3 How many open records requests regarding **PII** were referred to the Office of the Attorney General (OAG) for ruling during FY 2009? 1,247

Ques-4 Of those requests sent to the OAG (**Ques 3**), how many requests were ruled to be protected information (not for release under the Public Information Act)? 1,118

Ques-5 In your view, how often do the following request information from your division/program? Please rank in order of frequency assigning a 4 to the group that submits the most open record requests down to 1 being the group that submits the fewest open record requests. If other is identified, please include a ranking for that fifth grouping.

Rank

Individuals	1(24), 2(31), 3(51), 4(75), 5(3) = 554 (total score)
Legislature	1(111), 2(19), 3(15), 4(26), 5(1) = 303 (total score)
Media	1(30), 2(88), 3(54), 4(8), 5(1) = 405 (total score)
Businesses	1(24), 2(35), 3(54), 4(66), 5(2) = 530 (total score)
Other	1(1), 2(5), 3(5), 4(7), 5(5) = 79 (total score)

Ques-6 Does your agency/institution receive revenue (through cost recovery, subscriptions, websites, fees, etc.) for providing information?

[122] Yes [39] No [1] no response **(If No, go to Ques -9)**

Ques-7 What was the total revenue your agency/institution received for information provided for the following fiscal years:

FY 2005	\$60,890,818;
FY 2006	\$65,300,214;
FY 2007	\$66,101,091;
FY 2008	\$66,655,584;
FY 2009	\$65,531,339;

Ques-8 How much of the revenue listed in **Question 7** was for information provided under Transportation Code Chapters 521, 522 and 730:

FY 2005 \$53,712,892;

FY 2006 \$57,369,072;

FY 2007 \$57,445,278;

FY 2008 \$58,382,525;

FY 2009 \$58,070,717;

Ques-9 Have you received any request(s) from an individual not to share his/her PII?

[46] Yes [111] No [5] no response (*If NO*, go to **Ques-12**)

Ques-10 If **YES**, approximately, how many during the last 2 Years? 7,571

Ques-11 Would you please briefly explain the most recent request?

We would like to know your opinion in reference to the following topics. How do you rate the safety and security of PII in your division/program by marking [1] as the LOWEST (not at all secure) and [10] as the HIGHEST (very secure):

	Not Secure							Very Secure		
	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]	[10]
Ques-12 In reference to the way in which PII is collected/received?	[0]	[2]	[1]	[0]	[6]	[8]	[20]	[40]	[48]	[8]
	no response									
Ques-13 In reference to the way in which PII is stored/maintained?	[0]	[1]	[2]	[1]	[5]	[3]	[15]	[38]	[50]	[68]
	no response									
Ques-14 In reference to the way in which PII is transmitted to authorized recipients?	[0]	[1]	[0]	[2]	[5]	[6]	[17]	[44]	[56]	[8]
	no response									
Ques-15 In reference to the way in which PII is handled by staff responsible for managing it?	[1]	[0]	[0]	[0]	[2]	[4]	[15]	[38]	[56]	[66]
	no response									
Ques-16 In reference to requests for information from outside the agency ?	[0]	[0]	[1]	[1]	[2]	[4]	[16]	[37]	[55]	[64]
	no response									
Ques-17 In reference to sharing with other agencies/divisions?	[0]	[1]	[1]	[2]	[2]	[4]	[15]	[38]	[48]	[69]
	no response									
Ques-18 Is the subject of security and/or privacy of PII discussed in weekly or monthly meetings?	[48] Yes [100] No [34] Don't Know [9] no response									

Ques-19 Are there postings or announcements in the work area reminding staff of the need for safety/security of PII? [49] Yes [109] No [26] Don't Know [7] no response

Ques-20 In your view, do personnel receive adequate training in assuring safety and security of PII? [128] Yes [23] No [34] Don't Know [6] no response

Ques-21 In your view, what issues, if any, present a significant challenge in protecting PII data?

Comments:

**We wish to thank you for taking the time to assist us in gathering this information.
We will provide you with a link to the report when it has been completed and
published.**

Bidder/Contractor Data Questionnaire

Agency/Institution: 103 State Agencies 57 IHEs

Completed by: _____ Telephone No.: _____

E-mail: _____

Ques-1 Approximately how many new contractors and bidders are entered into your files and/or databases?

Number 114,213 per [56] Month [9] Quarter [91] Year

Ques-2 What was the total number of bidders/contractors (former or active) stored in your files and/or databases as of January 1, 2010 (all years) ? 4,207,106

Ques-3 What type of Information is collected from or about bidders/contractors by your agency/institution? (Please check all that apply)

- 163 a ☐ Name (First and Last)
- 102 b ☐ Social Security No.
- 12 c ☐ Date of Birth
- 5 d ☐ Birth Place
- 45 e ☐ Home Address
- 18 f ☐ Employment Data (hire date, salary, etc.)
- 4 g ☐ Mother's Maiden Name
- 45 h ☐ Personal E-mail Address
- 4 i ☐ Passport No.
- 47 j ☐ Personal Cell/Home Phone
- 132 k ☐ Texas Taxpayer ID No.
- 2 l ☐ Credit Card/Debit Card No.
- 51 m ☐ Banking Information (e.g., Account/Routing
- 7 n ☐ Finger Prints
- 9 o ☐ Handwriting/Sample Handwriting
- 0 p ☐ Medical Information
- 1 q ☐ Physically Impaired Information
- 10 r ☐ Photo (Electronic Image of Face)
- 0 s ☐ Retina or Iris Image
- 30 t ☐ Background Check/Criminal Record
- 1 u ☐ Substance Abuse Related Information
- 54 v ☐ Educational Background (Schools, degrees, etc.)
- 15 w ☐ Immigration, naturalization & citizenship
- 1 x ☐ Information about the Individual's Spouse
- 2 y ☐ Information about the Individual's Child(ren)
- 12 z ☐ Credit History
- 4 aa ☐ Motor Vehicle Information (license plate, reg.,
- 28 bb ☐ Tax Violations
- 5 cc ☐ Account No. and/or Login Information
- 74 dd ☐ Personal or Business Financial Statements
- 87 ee ☐ Names of employees
- 25 ff ☐ Accounting Records
- 69 gg ☐ Contracts
- 40 hh ☐ Customer List
- 9 ii ☐ Loan Information
- 22 jj ☐ Fed Income Tax Information
- 12 kk ☐ Lien Information
- 59 ll ☐ Bond Information
- 114 mm ☐ Federal Employment ID No.
- 4 nn ☐ Tax Preparer Information
- 20 oo ☐ Name and/or Information of previous business owner
- 16 pp ☐ Emergency Contact
- 16 qq ☐ Driving Records (driver's license, accident information, etc.)
- 82 rr ☐ Contract/Bid/Consultation History
- 96 ss ☐ Business Insurance info
- 96 tt ☐ Reference check

- 112 uu ☐ Qualification Information
 69 vv ☐ Capacity Information (Financial and Non-financial)
 112 ww ☐ Bid/Contract/Consultation Amount
 2 xx ☐ Birth Certificate
 36 yy ☐ Other (Please specify) _____

Ques-4 Of all the Personally Identifiable Information (PII) data which you have checked above, which information could you cease to collect without being detrimental to the functioning of your agency, division or program? Please identify them in the following space by corresponding letters such as k, n, aa, ... etc.

customer list/financial & non-financial capacity info (3); SSN/names of employees/personal e-mail address/
 personal phone/financial statements/names of employees (2); DOB/banking info/credit history/accounting records/loan
 info/driving records/business insurance info/reference checks/qualification info (1)

Ques-5 Do you ask your bidders/contractors to sign an agreement allowing the disclosure of Personally Identifiable Information (PII)?

[14] Yes [158] No (**If NO**, go to **Ques-7**)

If YES, please include a copy of the agreement with this questionnaire.

Ques-6 **If Yes**, is signing the agreement mandatory or voluntary?

[12] Mandatory [2] Voluntary

Ques-7 What is your agency's/institution's policy for sharing bidder/contractor information (Check all that apply)

- 27 ☐ There is a specific written policy against sharing PII
 56 ☐ There are general guidelines for sharing all types of PII
 0 ☐ Bidder/Contractor personal information is sold to private parties
 0 ☐ Bidder/Contractor personal information is sold to businesses
 16 ☐ Bidder/Contractor personal information is sold to or shared with other governmental entities
 96 ☐ Other (Please explain)

Ques-8 What is the agency's/institution's procedure for dealing with personal information relating to unsuccessful bids or contractors who are no longer providing services? (check all that apply)

- 40 ☐ Destroy/purge the information
 106 ☐ Keep the information in a central location
 34 ☐ Keep in the division which received contractor services
 34 ☐ Keep all information in an electronic/database format
 15 ☐ Keep certain information in an electronic/database format (list types of information): _____

- 55 ☐ Other (Please explain)

Ques-9 Have you received any request(s) from an individual not to share his/her PII?

[23] Yes [151] No (*If NO* , go to **Ques-12**)

Ques-10 **If YES**, approximately, how many during the last 2 Years? 128

Ques-11 Would you please briefly explain the most recent request?

We would like to know your opinion in reference to the following topics. How do you rate the safety and security of PII in your division/program by marking [1] as the LOWEST (not at all secure) and [10] as the HIGHEST (very secure):

	Not Secure										Very Secure									
	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]	[10]										
Ques-12 In reference to the way in which PII is collected/received?	[0]	[0]	[0]	[2]	[10]	[16]	[15]	[48]	[51]	[28]										
Ques-13 In reference to the way in which PII is stored/maintained?	[0]	[1]	[1]	[1]	[7]	[7]	[18]	[52]	[51]	[32]										
Ques-14 In reference to requests for information from outside the agency/institution?	[0]	[0]	[0]	[0]	[6]	[9]	[16]	[31]	[43]	[60]										
Ques-15 In reference to the way PII is transmitted to authorized recipients?	[0]	[0]	[0]	[1]	[6]	[9]	[14]	[38]	[47]	[50]										
Ques-16 In reference to the way PII is handled by those responsible for managing it?	[0]	[0]	[0]	[2]	[4]	[10]	[12]	[41]	[61]	[40]										
Ques-17 In reference to requests for information from outside the agency?	[1]	[0]	[0]	[1]	[4]	[9]	[11]	[24]	[41]	[44]										
Ques-18 In reference to sharing with other agencies/divisions?	[0]	[1]	[0]	[0]	[5]	[11]	[16]	[39]	[45]	[45]										
Ques-19 Is the subject of security and/or privacy of PII discussed in weekly or monthly meetings?											[49] Yes [97] No [25] Don't know									
Ques-20 Are there postings or announcements in the work area reminding staff of safety/security of PII?											[32] Yes [121] No [18] Don't know									
Ques-21 In your view, do personnel receive <u>adequate</u> training in safety and security of PII?											[119] Yes [32] No [19] Don't know									
Ques-22 In your view, what issues, if any, present a significant challenge in protecting PII data?																				

Comments

We wish to thank you for taking the time to assist us in gathering this information. We will provide you with a link to the report when it has been completed and published.

Appendix F:

Fifty States Comparison of Confidentiality of Date of Birth Records

Fifty State Comparison of Confidentiality of Date of Birth Records of State Government Employees

State	Status	Standard	Code/Statute	Exemption Language
Arizona	Protected	Personnel records	Ariz. Admin Code R2-5-105	F. Disclosure of information. The Director, or designee, shall ensure that except as provided in subsection (E), only the following information about an employee is provided to any person under A.R.S. Title 39, Chapter 1, Article 2. 1. Name of employee; 2. Date of employment; 3. Current and previous class titles and dates received;4. Name and location of current and previous agencies to which the employee has been assigned;5. Current and previous salaries and dates of each change; and 6. Name of employee's current or last known supervisor.
Delaware	Protected	Personnel records; invasion of personal privacy	Del. Code Title 29 Sec. 10002	(g) "Public record" is information of any kind, owned, made, used, retained, received, produced, composed, drafted or otherwise compiled or collected, by any public body, relating in any way to public business, or in any way of public interest, or in any way related to public purposes, regardless of the physical form or characteristic by which such information is stored, recorded or reproduced. For purposes of this chapter, the following records shall not be deemed public: (1) Any personnel, medical or pupil file, the disclosure of which would constitute an invasion of personal privacy, under this legislation or under any State or federal law as it relates to personal privacy
Georgia	Protected	Date of birth specifically protected	Ga. Code Sec. 50-18-72 11.3(A)	(11.3) (A) An individual's social security number, mother's birth name, credit card information, debit card information, bank account information, financial data or information, and insurance or medical information in all records, and if technically feasible at reasonable cost, day and month of birth, which shall be redacted prior to disclosure of any record requested pursuant to this article; provided, however, that such information shall not be redacted from such records if the person or entity requesting such records requests such information in a writing signed under oath by such person or a person legally authorized to represent such entity which states that such person or entity is gathering information as a representative of a news media organization for use in connection with news gathering and reporting; and provided, further, that such access shall be limited to social security numbers and day and month of birth; and provided, further, that this news media organization exception for access to social security numbers and day and month of birth and the other protected information set forth in this subparagraph shall not apply to teachers, employees of a public school, or public employees as set forth in paragraph (13.1) of this subsection. For purposes
Hawaii	Protected	Unwarranted invasion of personal privacy	HI Rev. Stat. Sec. 92F-13	Government records; exceptions to general rule. This part shall not require disclosure of: (1) Government records which, if disclosed, would constitute a clearly unwarranted invasion of personal privacy
Idaho	Protected	Date of birth specifically protected	Idaho Code Title 9, Evidence, Ch. 3, Public Writings, 9-340C	The following records are exempt from disclosure: (1) Except as provided in this subsection, all personnel records of a current or former public official other than the public official's public service or employment history, classification, pay grade and step, longevity, gross salary and salary history, status, workplace and employing agency. All other personnel information relating to a public employee or applicant including, but not limited to, information regarding sex, race, marital status, birth date, home address and telephone number, applications, testing and scoring materials, grievances, correspondence and performance evaluations, shall not be disclosed to the public without the employee's or applicant's written consent.
Illinois	Protected	Unwarranted invasion of personal privacy	IL. Gen. Provisions Ch. 5 ILCS 140 Sec. 7 (b)	(b) Information that, if disclosed, would constitute a clearly unwarranted invasion of personal privacy, unless the disclosure is consented to in writing by the individual subjects of the information. The disclosure of information that bears on the public duties of public employees and officials shall not be considered an invasion of personal privacy. Information exempted under this subsection (b) shall include but is not limited to: (ii) personnel files and personal information maintained with respect to employees, appointees or elected officials of any public body or applicants for those positions.
Iowa	Protected	Personnel records	Iowa Code Sec. 22.7	11. Personal information in confidential personnel records of public bodies including but not limited to cities, boards of supervisors and school districts.
Kansas	Protected	Personnel records; Unwarranted invasion of personal privacy	Kan. Statute Sec. 45-221	(4) Personnel records, performance ratings or individually identifiable records pertaining to employees or applicants for employment, except that this exemption shall not apply to the names, positions, salaries or actual compensation employment contracts or employment-related contracts or agreements and lengths of service of officers and employees of public agencies once they are employed as such.

Fifty State Comparison of Confidentiality of Date of Birth Records of State Government Employees

State	Status	Standard	Code/Statute	Exemption Language
Kentucky	Protected	Unwarranted invasion of personal privacy	Ky. Rev. Stat. Sec. 61.878(1)(a)	(a) Public records containing information of a personal nature where the public disclosure thereof would constitute a clearly unwarranted invasion of personal privacy;
Maryland	Protected	Personnel records	Md. State Govt. Code Sec. 10-616 (i)(1)	(i) Personnel Records – (1) Subject to paragraph (2) of this section, a custodian shall deny inspection of a personnel record of an individual, including an application, performance rating, or scholastic achievement information. (2) A custodian shall permit inspection by: (i) the person in interest; or (ii) an elected or appointed official who supervises the work of the individual.
Massachusetts	Protected	Unwarranted invasion of personal privacy	Mass. Gen. Laws Ch. 4 Sec. 7 26th	(c) personnel and medical files or information; also any other materials or data relating to a specifically named individual, the disclosure of which may constitute an unwarranted invasion of personal privacy
Michigan	Protected	Unwarranted invasion of personal privacy	Mich. Comp. Laws Sec. 15.243	(1) A public body may exempt from disclosure as a public record under this act any of the following: (a) Information of a personal nature if public disclosure of the information would constitute a clearly unwarranted invasion of an individual's privacy.
Mississippi	Protected	Personnel records	Miss. Code Sec. 25-1-100	(1) Personnel records and applications for employment in the possession of a public body, as defined by paragraph (a) of Sec. 25-61-3, except those which may be released to the person who made the application or with the prior written consent of the person who made the application, shall be exempt from the provisions of the Mississippi Public Records Act of 1983.
New Hampshire	Protected	Unwarranted invasion of personal privacy	Nh. Rev. Stat. Sec. 91-A:5	IV. Records pertaining to internal personnel practices; confidential, commercial, or financial information; test questions, scoring keys, and other examination data used to administer a licensing examination, examination for employment, or academic examinations; and personnel, medical, welfare, library user, videotape sale or rental, and other files whose disclosure would constitute invasion of privacy.
New Jersey	Protected	Unwarranted invasion of personal privacy	N.J. Stat. Sec. 47:1A-10	11. Notwithstanding the provisions of P.L.1963, c.73 (C.47:1A-1 et seq.) or any other law to the contrary, the personnel or pension records of any individual in the possession of a public agency, including but not limited to records relating to any grievance filed by or against an individual, shall not be considered a government record and shall not be made available for public access, except that: an individual's name, title, position, salary, payroll record, length of service, date of separation and the reason therefor, and the amount and type of any pension received shall be a government record; personnel or pension records of any individual shall be accessible when required to be disclosed by another law, when disclosure is essential to the performance of official duties of a person duly authorized by this State or the United States, or when authorized by an individual in interest
New York	Protected	Unwarranted invasion of personal privacy	N.Y. Pub. Off. Law Art. 6 Sec. 89(2)(b)	(b) An unwarranted invasion of personal privacy includes, but shall not be limited to: i. disclosure of employment, medical or credit histories or personal references of applicants for employment; ii. disclosure of items involving the medical or personal records of a client or patient in a medical facility; iii. sale or release of lists of names and addresses if such lists would be used for commercial or fund-raising purposes; iv. disclosure of information of a personal nature when disclosure would result in economic or personal hardship to the subject party and such information is not relevant to the work of the agency requesting or maintaining it; v. disclosure of information of a personal nature reported in confidence to an agency and not relevant to the ordinary work of such agency; or vi. information of a personal nature contained in a workers' compensation record, except as provided by section one hundred ten-a of the workers' compensation law.
North Carolina	Protected	Date of birth specifically protected	Nc. Stat. Sec. 132-1.2	132-1.2. Confidential information. Nothing in this Chapter shall be construed to require or authorize a public agency or its subdivision to disclose any information that: (1) Meets all of the following conditions: a. Constitutes a "trade secret" as defined in G.S. 66-152(3). b. Is the property of a private "person" as defined in G.S. 66-152(2). c. Is disclosed or furnished to the public agency in connection with the owner's performance of a public contract or in connection with a bid, application, proposal, industrial development project, or in compliance with laws, regulations, rules, or ordinances of the United States, the State, or political subdivisions of the State. d. Is designated or indicated as "confidential" or as a "trade secret" at the time of its initial disclosure to the public agency... (4) Reveals the electronically captured image of an individual's signature, date of birth, drivers license number, or a portion of an individual's social security number if the agency has those items because they are on a voter registration document.

Fifty State Comparison of Confidentiality of Date of Birth Records of State Government Employees

State	Status	Standard	Code/Statute	Exemption Language
North Dakota	Protected	Personnel records	N.D. Cent. Code Sec. 44-04-18.1	2. Except as otherwise specifically provided by law, personal information regarding a public employee contained in an employee's personnel record or given to the state or a political subdivision by the employee in the course of employment is exempt. As used in this section, "personal information" means a person's home address; home telephone number; photograph; medical information; motor vehicle operator's identification number; payroll deduction information; the name, address, telephonenumber, and date of birth of any dependent or emergency contact; any credit, debit, or electronic fund transfer card number; and any account number at a bank or other financial institution.
Oregon	Protected	Personnel records	Or. Rev. Stat. Sec. 192.502(3)*	The following public records are exempt from disclosure under ORS 192.410 to 192.505: (3) Public body employee or volunteer addresses, Social Security numbers, dates of birth and telephone numbers contained in personnel records maintained by the public body that is the employer or the recipient of volunteer services. This exemption: (a) Does not apply to the addresses, dates of birth and telephone numbers of employees or volunteers who are elected officials, except that a judge or district attorney subject to election may seek to exempt the judge's or district attorney's address or telephone number, or both, under the terms of ORS 192.445; (b) Does not apply to employees or volunteers to the extent that the party seeking disclosure shows by clear and convincing evidence that the public interest requires disclosure in a particular instance; (c) Does not apply to a substitute teacher as defined in ORS 342.815 when requested by a professional education association of which the substitute teacher may be a member; and (d) Does not relieve a public employer of any duty under ORS 243.650 to 243.782.
Rhode Island	Protected	Personnel records	R.I. Gen. Laws Sec. 38-2-2	The following records shall not be deemed public: (A) All records which are identifiable to an individual applicant for benefits, client, patient, student, or employee, including, but not limited to, personnel, medical treatment, welfare, employment security, pupil records, all records relating to a client/attorney relationship and to a doctor/patient relationship, and all personal or medical information relating to an individual in any files, including information relating to medical or psychological facts, personal finances, welfare, employment security, student performance, or information in personnel files maintained to hire, evaluate, promote, or discipline any employee of a public body; provided, however, with respect to employees, the name, gross salary, salary range, total cost of paid fringe benefits, gross amount received in overtime, and other remuneration in addition to salary, job title, job description, dates of employment and positions held with the state or municipality, work location, business telephone number, the city or town of residence, and date of termination shall be public.
South Carolina	Protected	Unreasonable invasion of personal privacy	SC Code Sec. 30-4-40(a)(2)	(a) A public body may but is not required to exempt from disclosure the following information: (2) Information of a personal nature where the public disclosure thereof would constitute unreasonable invasion of personal privacy. Information of a personal nature shall include, but not be limited to, information as to gross receipts contained in applications for business licenses and information relating to public records which include the name, address, and telephone number or other such information of an individual or individuals who are handicapped or disabled when the information is requested for person-to-person commercial solicitation of handicapped persons solely by virtue of their handicap. This provision must not be interpreted to restrict access by the public and press to information contained in public records.

Fifty State Comparison of Confidentiality of Date of Birth Records of State Government Employees

State	Status	Standard	Code/Statute	Exemption Language
Utah	Protected	Unwarranted invasion of personal privacy	Utah Code Sec 63-2-302(2)(d)	(2) The following records are private if properly classified by a governmental entity: (a) records concerning a current or former employee of, or applicant for employment with a governmental entity, including performance evaluations and personal status information such as race, religion, or disabilities, but not including records that are public under Subsection 63-2-301(2)(b) or 63-2-301(3)(o), or private under Subsection (1)(b); (b) records describing an individual's finances, except that the following are public: (i) records described in Subsection 63-2-301(2); (ii) information provided to the governmental entity for the purpose of complying with a financial assurance requirement; or (iii) records that must be disclosed in accordance with another statute; (c) records of independent state agencies if the disclosure of those records would conflict with the fiduciary obligations of the agency; (d) other records containing data on individuals the disclosure of which constitutes a clearly unwarranted invasion of personal privacy; and (e) records provided by the United States or by a government entity outside the state that are given with the requirement that the records be managed as private records, if the providing entity states in writing that the record
Virginia	Protected	Personnel records	Va. Code Sec. 2.2-3705.1(1)	The following records are excluded from the provisions of this chapter but may be disclosed by the custodian in his discretion, except where such disclosure is prohibited by law: 1. Personnel records containing information concerning identifiable individuals, except that access shall not be denied to the person who is the subject thereof. Any person who is the subject of any personnel record and who is 18 years of age or older may waive, in writing, the protections afforded by this subdivision. If the protections are so waived, the public body shall open such records for inspection and copying.
Washington	Protected	Unwarranted invasion of personal privacy	Wa. Rev. Code Sec. 42.65.230	The following personal information is exempt from public inspection and copying under this chapter: (1) Personal information in any files maintained for students in public schools, patients or clients of public institutions or public health agencies, or welfare recipients; (2) Personal information in files maintained for employees, appointees, or elected officials of any public agency to the extent that disclosure would violate their right to privacy
Wyoming	Protected	Personnel records	Wyo. Stat. Sec. 16-4-203 (d) (iii)	(d) The custodian shall deny the right of inspection of the following records, unless otherwise provided by law: (iii) Personnel files except those files shall be available to the duly elected and appointed officials who supervise the work of the person in interest. Applications, performance ratings and scholastic achievement data shall be available only to the person in interest and to the duly elected and appointed officials who supervise his work. Employment contracts, working agreements or other documents setting forth the terms and conditions of employment of public officials and employees are not considered part of a personnel file and shall be available for public inspection

Fifty State Comparison of Confidentiality of Date of Birth Records of State Government Employees

State	Status	Standard	Code/Statute	Exemption Language
Arkansas	Not Specifically Protected	Personal records	Ar. Code Sec. 25-19-105 (b)	(b) It is the specific intent of this section that the following shall not be deemed to be made open to the public under the provisions of this chapter: (10) Personnel records to the extent that disclosure would constitute clearly unwarranted invasion of personal privacy.
California	Not Specifically Protected	Unwarranted invasion of personal privacy	Ca. Govt. Code Sec. 6254	6254. Except as provided in Sections 6254.7 and 6254.13, nothing in this chapter shall be construed to require disclosure of records that are any of the following: (c) Personnel, medical, or similar files, the disclosure of which would constitute an unwarranted invasion of personal privacy.
Connecticut	Not Specifically Protected	Unwarranted invasion of personal privacy	Ct. Gen. Statutes Sec. 1-210	(a) Except as otherwise provided by any federal law or state statute, all records maintained or kept on file by any public agency, whether or not such records are required by any law or by any rule or regulation, shall be public records and every person shall have the right to (1) inspect such records promptly during regular office or business hours, (2) copy such records in accordance with subsection (g) of section 1-212, or (3) receive a copy of such records in accordance with section 1-212. Any agency rule or regulation, or part thereof, that conflicts with the provisions of this subsection or diminishes or curtails in any way the rights granted by this subsection shall be void. Each such agency shall keep and maintain all public records in its custody at its regular office or place of business in an accessible place and, if there is no such office or place of business, the public records pertaining to such agency shall be kept in the office of the clerk of the political subdivision in which such public agency is located or of the Secretary of the State, as the case may be. Any certified record hereunder attested as a true copy by the clerk, chief or deputy of such agency or by such other person designated or empowered by law to so act, shall be competent evidence in any court of this state of the facts contained therein. (b) Nothing in the Freedom of Information Act shall be construed to require disclosure of: (2) Personnel or medical files and similar files the disclosure of which would constitute an invasion of personal
Nebraska	Not Specifically Protected	Personal records	NE Rev. Stat. Sec. 84-712.05(7)	The following records, unless publicly disclosed in an open court, open administrative proceeding, or open meeting or disclosed by a public entity pursuant to its duties, may be withheld from the public by the lawful custodian of the records: (7) Personal information in records regarding personnel of public bodies other than salaries and routine directory information;
Texas	Not Specifically Protected	Personal Records	TX Govt. Code Section 552.022 (A) (2)	(a) Without limiting the amount or kind of information that is public information under this chapter, the following categories of information are public information and not excepted from required disclosure under this chapter unless they are expressly confidential under other law: (2) the name, sex, ethnicity, salary, title, and dates of employment of each employee and officer of a governmental body;
Alabama, Alaska, Colorado, Florida, Indiana, Louisiana, Maine, Minnesota, Missouri, Montana, Nevada, New Mexico, Ohio, Oklahoma, Pennsylvania, South Dakota, Tennessee, Vermont, Washington, D.C., West Virginia, and Wisconsin	Not Specifically Protected			